НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК _____

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___” _____ 2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 «Прикладна математика» _____
(код і назва)

на тему: Побудова розпізнавачів на відкритих ключах для «Калина»-подібних шифрів _____

Виконав (-ла): студент (-ка) 2__ курсу, групи ФІ-73 мп
(шифр групи)

Коляда Марія Олександрівна _____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник доцент, к.т.н. Яковлєв С.В _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти: другий (магістерський) за освітньо–професійною програмою

Спеціальність: 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
«___»_____201_ р.

ЗАВДАННЯ
на магістерську дисертацію студенту

Коляда Марія Олександрівна
(прізвище, ім'я, по батькові)

1. Тема дисертації: Побудова розпізнавачів на відкритих ключах для «Калина»-подібних шифрів _____
_____,
науковий керівник дисертації: Яковлєв Сергій Володимирович доцент, к.т.н. ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____р. № _____

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження: інформаційні процеси в системах криптографічного захисту _____

4. Предмет дослідження (Вхідні дані – для магістерської дисертації за освітньо–професійною програмою):
криптографічні властивості <<Калина>>-подібних шифрів _____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____
_____

6. Орієнтовний перелік ілюстративного матеріалу _____

_____

_____

7. Орієнтовний перелік публікацій _____

_____

_____

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Роботу виконано на 63 аркушах, перелік посилань на використані джерела з 12 найменувань. У роботі наведено 16 рисунків та 3 таблиць.

У даній роботі було побудовано моделі розпізнавача із відомим ключем. Було розглянуто основні поняття для побудови моделі розпізнавача із відомим ключем та сценарії роботи для розпізнавача на прикладі застосування даної техніки до блокового шифру AES.

Надалі було розглянуто модифікацію блокового шифру «Калина» та застосовано до нього техніку побудови моделі розпізнавача із відомим ключем. Як результат, було побудовано три моделі розпізнавача із відомимключем та сценарії роботи для елементів розпізнавача для 5 та 7 раундів шифрування.

На основі отриманих результатів було проведено дослідження щодо впливу раундових перетворень «Калина»-подібних шифрів на структуру певних підпрострів відкритих текстів та побудовано розпізнавач для «Калина»-подібних шифрів.

Метою даної дипломної роботи є розробка та імплементація нових алгебраїчних методів криптоаналізу блокових шифрів.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є криптографічні властивості «Калина»-подібних шифрів.

В ході дослідження було побудовано модель розпізнавача із відомим ключем, що використовує властивості ланцюгів підросторів. Сформульовано вигришні сценарії для елементів розпізновача із відомим ключем для «Калина»-подібних шифрів.

ПІДПРОСТІР, ЛАНЦЮГ, СИМЕТРИЧНІ БЛОКОВІ ШИФРИ, РОЗПІЗНАВАЧ НА ВІДОМИХ КЛЮЧАХ

РЕФЕРАТ

Дипломная работа выполнена на 63 листах, она содержит список ссылок на использованные источники с 12 наименований. В работе приведены 16 рисунков и 3 таблиц.

В данной работе было построено модели распознавателя на известных ключах. Были рассмотрены основные понятия для построения распознавателя с известным ключом и сценарии работы для распознавателя на примере применения данной техники к блочному шифру AES.

Далее было рассмотрено модификацию блочного шифра «Калина» и применено к нему технику построения распознавателя с известным ключом. В результате, было построено три модели распознавателя с известным ключом и сценарии работы для его элементов для 5 и 7 раундов шифрования.

Целью данной дипломной работы является разработка и имплементация новых алгебраических методов криптоанализа блочных шифров.

Объектом исследования является информационные процессы в системах криптографической защиты.

Предметом исследования является криптографические свойства «Калина»-подобных шифров.

В ходе исследования было построено модель распознавателя с известным ключом, который использует свойства цепей подпространств. Было сформулировано выигрышные сценарии для элементов распознавателя с известным ключом для «Калина»-подобных шифров.

ПОДПРОСТРАНСТВО, ЦЕПЬ, СИММЕТРИЧЕСКИЕ БЛОЧНЫЕ ШИФРЫ, РАСПОЗНАВАТЕЛЬ С ИЗВЕСТНЫМ КЛЮЧОМ

ABSTRACT

The thesis is presented in 63 pages. It contains bibliography of 12 references. 16 figures and 3 tables are given in the thesis.

In this work we constructed of Known-Key Distinguishers. We reviewed the main terms for constructing of Known-Key Distinguishers and The Known-Key Distinguisher Scenario. Like example we reviewed implementation of this technique to AES block cipher.

The next step we reviewed modification of «Kalyna» block cipher and construct Known-Key Distinguishers. As result, we created 3 types of Known-Key Distinguishers and the Known-Key Distinguisher Scenarios for 5-7 cipher rounds.

The object is information processes in cryptographic security systems.

The subject is cryptographic properties of «Kalyna»-type ciphers.

As a part of the study we had constructed 3 types of Known-Key Distinguishers, that based on subspace trails for block ciphers, created Scenarios for elements of the Known-Key Distinguisher for «Kalyna»-type ciphers.

SUBSPACE, TRAIL, SYMMETRIC BLOCK CIPHERS, KNOWN-KEY DISTINGUISHER

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

$\oplus$ — операція побітового додавання

$R^{(i)}$ - визначає процедуру зашифрування i раундів «Калини» або AES

$SubBytes(S-Box)$ – нелінійна операція в шифрі(застосування кожних 8 біт відкритого тексту до 8 біт $S-Box$, операція проводиться 16 разів).

$ShiftRows(SR)$ – циклічний зсув.

$MixColumns(MC)$ – множення кожного стовпчика на константну матрицю

ВСТУП

Актуальність дослідження. У сьогоденні існує велика кількість блокових шифрів, котрі використовуються для шифрування великих об'ємів інформації. Одним з найвідоміших та найбільш шикоро використовуваних є блоковий шифр AES. За для безпечого використання шифру, ми завжди повинні пам'ятати про стійкість шифру до атак. Як відомо, ідеальний шифр не має відрізнятися від випадкової перестановки. Якщо ж за певних умов шифр не веде себе я випадкова перестановка, це означає що при шифруванні зловмисник може передбачити результат та скористатися даною вразливістю. Одним нових методів криптоаналізу блокових шифрів є аналіз ланцюгів підпросторів підібраних спеціальним чином. За допомогою даного методу ми можемо побудувати модель розпізнавача із відомим ключем, котра доводить що за певних умов шифр не веде себе як випадкова перестановка. Оскільки наш державний стандарт блокового шифрування «Калина» має подібну до AES структуру, то дуже важливо знати, чи можливо побудувати розпізнавач із відомим ключем для нього. В свою чергу, вдала побудова розпізнавача буде означати, що за певних обмежень даний шифр буде відрізнятися від випадкової перестановки.

Метою дослідження є розробка та імплементація нових алгебраїчних методів криптоаналізу блокових шифрів. **Задача дослідження** полягає у застосуванні нового методу криптоаналізу, що використовує ланцюги підпросторів, при побудові моделі розпізнавача із відомим ключем до «Калина» - подібних шифрів. Для розв'язання задачі необхідно вирішити такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) дослідити збереження властивостей збалансованості та збереження рівномірного розподілу для раундових перетворень «Калина»-подібних шифрів;

3) розширити побудовані ланцюги підпросторів;

4) використовуючи побудовані ланцюги підпросторів, побудувати модель розпізнавача із відомим ключем для «Калина»-подібних шифрів.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є криптографічні властивості «Калина»-подібних шифрів.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи лінійної та абстрактної алгебри, теорії імовірностей, математичної статистики, комбінаторного аналізу.

Наукова новизна. Вперше для «Калина»-подібних шифрів було побудовано модель розпізнавача із відомим ключем.

Практичне значення. Побудова моделі розпізнавача на відомих ключах дозволить довести, що за певних обмежень «Калина»-подібні шифри не ведуть себе як випадкова перестановка. Це означає, що дана властивість може бути використана в методах практичного криптоаналізу «Калина»-подібних шифрів.

1 ОГЛЯД ТА ОПИС МЕТОДУ КРИПТОАНАЛІЗУ ІЗ ВІДОМИМ КЛЮЧЕМ

1.1 Модель криптоаналізу із відомим ключем

Модель криптоаналізу із відомим ключем для блокових шифрів походить від криптоаналізу геш функцій, що був вперше запропонований Кнудсеном та Рюменом [9]. Головна відмінність даної моделі від звичайної полягає в наступному:

– у звичайній моделі зловмисник має чорний ящик (оракул), котрий не має повного доступу до шифруючої функції асоційованої із секретним ключем та її інверсії. Задача "чорного ящика": або знайти ключ, якщо шифр доступний у вигляді чорного ящика, або маючи чорний ящик сказати що всередині нього, тобо в даному випадку ефективно відрізняти шифртекст від випадкової послідовності.

– у моделі із відомим ключем зловмисник має білий ящик, котрий має повний доступ до шифруючої функції асоційованої з відомим випадковим ключем та її інверсії. Задача білого ящика: маючи можливість контролювати входи та виходи шифруючої функції, знайти кореляцію між ними. Білий ящик не зможе досягти цілі лише у тому випадку, коли буде мати справу із ідеально випадковою послідовністю. У такому випадку він буде однакові можливості із чорним ящиком.

Дамо більш детальні визначення, необхідні для побудови розпізнавача із відомим ключем, котрі були запропоновані Лоренсо Грасі та його колегами [6]:

Визначення 1.1. *T-складне відношення (T-intractable relatively)*: Нехай відображення $E : \{0,1\}^k * \{0,1\}^n \to \{0,1\}^n, (K,X) \to E_K(X)$ є блоковим шифром розміра n біт. Нехай $N \geqslant 1$ та R - натуральне число та довільне відношення над набором з S підпросторів по N елементів, що складаються з n-бітних блоків. Алгоритм A' конструює два підпростори,

що складаються з N елементів $x' = (X'_i)$ та $y' = (Yi_i)$ такі що $Y'_i = \Pi(X'_i)$ та $x'Ry'$ із ймовірністю успіху $p \leqslant \frac{1}{2}$, де П- випадково вибрана перестановка. Відношення R називається *T-складним відносно E*, якщо будь-який алгоритм A', виконується за час $T' \leqslant T$, де T'- дорівнює кількості обчислень над E.

Домовимося, що час необхідний для одного запиту до оракулу для отримання перестановки або її інверсії - рівний.

Визначення 1.2. *Розпізнавач із відомим ключем (known-key distinguisher)*:

Нехай відображення: $E : \{0,1\}^k * \{0,1\}^n \to \{0,1\}^n$,$(K,X) \to E_K(X)$ є блоковим шифром розміра n біт. *Розпізнавачем із відомим ключем* назвемо пару (R,A) порядка $N \geqslant 1$, що складається з відношення R та алгоритма A. R - відношення над набором підпросторів по N елементів по n біт. Алгоритм A - на вході приймає k-бітний ключ K, за час T_A розраховує пару $x' = (X'_i)$ - над відкритим текстом та $y' = (Y'_i)$ над шифртекстом над E, такі що $Y'_i = E_K(X'_i)$, та обов'язково виконуються наступні умови:

1) Відношення R має бути T_A - складним по відношенню до E

2) Перевірка виконуваності відношення R має бути ефективно-перевіряємою - тобто не перевищувати T_A операцій.

Зауважимо, що поки алгоритм A приймає на вхід випадковий ключ K, набори: вхід та вихід алгоритмів A або A', задовольняють відношенню R, однаково для всіх значень K та мають бути ефективно перевірятися без знання K.

1.2 Сценарій роботи розпізнавача із відомим ключем

У даному сценарії приймають участь наступні елементи: *генератор ключей (Key Generator), оракул (Oracle), чарівний гравець (Shortcut player), звичайний гравець (Generic player), валідатор (Verifier).*

Чарівний гравець - виконує роль білого ящика, котрий знає ключ, працює з алгоритмом A. *Звичайний гравець* - не знає ключа, має зробити запит до оракулу, щоб отримати шифртекст. Оракул може генерувати шифртекст, використовуючи випадкову перестановку замість процесу шифрування. *Валідатор* - запобігає шахраювання від обох сторін.

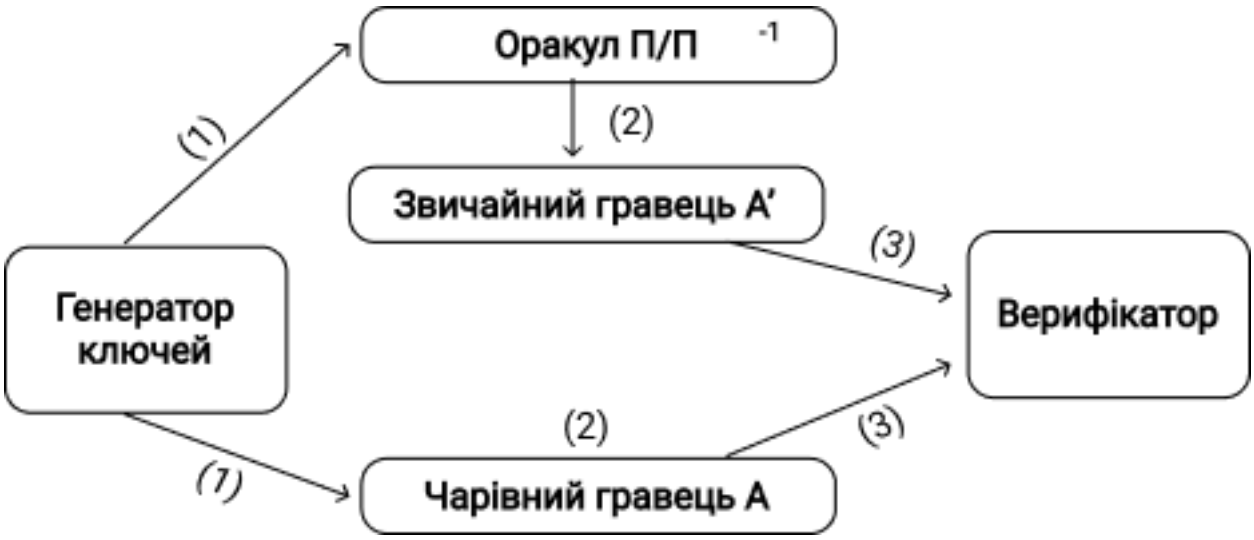

Рисунок 1.1 – Схема роботи розпізнавача

Сценарій роботи роботи розпізнавача полягає у виконанні наступних кроків:

1) Обирається відношення R

2) Генератор ключей генерує ключ, котрий подається на вхід оракулу та чарівному гравцю.

3) Чарівний гравець та звичайний гравець генерують пару над набором кортежів з N елементів по n біт (відкритий текст та шифртекст), котрі задовольняють відношенню R.

4) Валідатор робить наступну перевірку: чи задовільняє згенерована пара відношенню R?

5) Перемагає гравець, котрий швидше надіслав кортежі з N елементів по n біт, котрі задовольняють відношенню R.

Визначимо складність розпізнавача як суму складностей перевірок та конструювань пар відкритого тексту та шифртексту, котрі задовольняють заданим вимогам.

Зазначимо, що відношення R є ефективно перевіряємим тоді і тільки тоді, коли обчислювальна складність валідатора незначна порівняно з будь-ким із гравців.

Розпізнавач має сенс в тому випадку, коли складність роботи звичайного гравця (вартість одного звертання до оракулу, що дорівнює складності одного шифрування - генерації пари кортежів з N елементів по n біт) вища, ніж складність чарівного гравця. Тобто, коли ймовірність, що чарівний гравець буде переможцем вища, ніж коли звичайний гравець.

Розглянемо можливі варіанти оцінки складності роботи розпізнавача та проаналізуємо їх. Оскільки успіх роботи звичайного гравця залежить від згенерованих оракулом N-підпросторів (окремо від оракула звичайний гравець не може функціонувати), можливі наступні варіанти:

1) Складність обчислень для звичайного гравця визнається виключно кількістю звернень до оракулу.

2) Складність обчислень для звичайного гравця визначається, враховуючи кількість запитів гравця до оракулу та складність всіх інших обчислень гравця (у більшості випадків вона є незначною).

Інтуїтивно зрозуміло, що другий варіант оцінки є слабшим, але не завжди. Іноді бувають випадки, коли генерація ключа або проведення запиту до оракулу є складнішими. Але, у більшості випадків складність

обчислень звичайного гравця добре апроксимується кількістю запитів до оракулу. Тому, ми будемо розглядати саме такий варіант.

Для правильного проведення даного сценарію важливо розуміти, якими метриками оцінювати успіх гравців. Можливі наступні випадки:

1) Зафіксувати складність обчислень для кожного з гравців. В такому випадку, ми маємо оцінювати ймовірність перемоги гравців.

2) Для кожного з гравців зафіксувати ймовірність успіхів. В такому випадку, ми маємо оцінювати складність обчислень кожного з гравців, за якої він буде перемагати із заданою ймовірністю.

В даній роботі буде оцінюватися складність обчислень кожного з гравців.

1.3 AES (Advanced Encryption Standard)

AES [10] – це SP-мережа, котра підтримує ключі довжини 128,192 и 256 біт. 128-бітний відкритий текст подається у вигляді матриці $4 * 4$, кожна комірка котрої містить 8 біт, всі розрахунки ведуться над полем F_{256} за означенням використовуючи незвідний поліном $x^8 + x^4 + x^3 + x + 1$. В залежності від версії AES використовується різна кількість раундів N_r. Може бути рівним 10, 12 або 14 для AES-128, 192 і 256 відповідно. Раундові операції:

– $SubBytes(S - Box)$ – нелінійна операція в шифрі(застосування кожних 8 біт відкритого тексту до 8 біт $S - Box$, операція проводиться 16 разів).

– $ShiftRows(SR)$ – циклічний зсув.

– $MixColumns(MC)$ – множення кожного стовпчика на константну матрицю $4 * 4$ над GF_2.

– $AddRoundKey(ARK)$ – XOR з раундовим ключем.

Один раунд AES можливо описати функцією

$$R(x) = K \oplus MC \circ SR \circ S - box(x)$$

В першому блоці операція $AddRoundKey$ виконується, і в останньому раунді не виконується $MixColumns$.

Розглянемо алгоритм генерації ключів для AES-128. Простір раундових ключів позначимо як $W[0,...,43]$ де $W[.]$ містить 32 біта. Перших 4 позиції в $W[.]$ – це секретний ключ користувача. Інші раундові ключі розраховуються за правилом:

– Якщо $i \equiv 0 \mod 4$, то:

$$W[i] = W[i-4] \oplus RotByte(S - box(W[i-1])) \oplus RCON([i/4]).$$

– Інакше $W[i] = W[i-1] \oplus W[i-4]$.

Де $i = 4,...,43$, $RotByte$ - зсув 8 біт вліво, $RCON$ - массив наперед визначених констант.

1.4 Визначення та побудова ланцюгів підпросторів для AES

Нехай F раундова функція в ітеративному блочному шифрі зі змінним ключем [2]:

$$E_K(m) = k_n \oplus F(...F(k_1 \oplus F(k_0 \oplus m))),$$

де k_i – раунові ключі, отримані з основного ключа K використовуючи ключовий розклад:

$$f(k_0,...k_n) = f(K).$$

Нехай існує подпростір $V \oplus a$, такий що $F(V \oplus a) = V \oplus a'$. Тоді, якщо раундовий ключ K міститься в $V \oplus (a \oplus a')$, то з цього випливає, що $F(V \oplus a)K = V \oplus a$ та ми отримали ітеративний інваріантний простір.

Для довільного початкового підпростору $V \oplus a$ ми можемо поставити в відповідність інший $V \oplus b$, де b залежить від , та від раундового ключа, тобто для пари підпросторів V_1 та V_2 виконується: $F(V_1 \oplus a) \oplus K = V_2 \oplus b$.

Визначення 1.3. *Ланцюг просторів довжини* r – це простий кортеж $r + 1$ просторів $(V_1, V_2, ...V_{r+1})$, для котрих виконується $F(V_i \oplus a) \oplus K \subseteq V_{i+1} \oplus a_{i+1}$.

Надалі ми визначимо 4 сімейства підпросторів *діагональний простір, інверсійовано-діагональний простір, стовпчиковий простір* та *змішанний простр.*

Визначення 1.4. *Стовпчиковий простір* C_i визначимо наступним чином: $C_i = \langle e_{0,i}, e_{1,i}, e_{2,i}, e_{3,i} \rangle$. Наприклад, C_0 буде мати наступний вигляд:

$$C_0 = \left\{ \begin{bmatrix} \mathrm{x}_1 & 0 & 0 & 0 \\ \mathrm{x}_2 & 0 & 0 & 0 \\ \mathrm{x}_3 & 0 & 0 & 0 \\ \mathrm{x}_4 & 0 & 0 & 0 \end{bmatrix} | \forall x_1, x_2, x_3, x_4 \in F_{2^8} \right\}$$

Визначення 1.5. *Діагональний простір* D_i визначимо наступним чином: $D_i = SR^{-1}(C_i) = \langle e_{0,i}, e_{1,i+1}, e_{2,i+2}, e_{3,i+3} \rangle$, де індекс $i + j$ розраховується за модулем 4. Наприклад, D_0 буде мати наступний вигляд:

$$D_0 = \left\{ \begin{bmatrix} \mathrm{x}_1 & 0 & 0 & 0 \\ 0 & \mathrm{x}_2 & 0 & 0 \\ 0 & 0 & \mathrm{x}_3 & 0 \\ 0 & 0 & 0 & \mathrm{x}_4 \end{bmatrix} | \forall x_1, x_2, x_3, x_4 \in F_{2^8} \right\}$$

Визначення 1.6. *Інверсійовано-діагональний простір* ID_i визначимо наступним чином: $D_i = SR(C_i) = \langle e_{0,i}, e_{1,i-1}, e_{2,i-2}, e_{3,i-3} \rangle$, де індекс $i - j$

розраховується за модулем 4. Наприклад, ID_0 буде мати вигляд:

$$ID_0 = \left\{ \begin{bmatrix} \mathrm{x}_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathrm{x}_2 \\ 0 & 0 & \mathrm{x}_3 & 0 \\ 0 & \mathrm{x}_4 & 0 & 0 \end{bmatrix} | \forall x_1, x_2, x_3, x_4 \in F_{2^8} \right\}$$

Визначення 1.7. *Змішаний простір* M_i визначимо наступним чином: $M_i = MC(ID_i)$. Наприклад, M_0 буде мати вигляд:

$$M_0 = \left\{ \begin{bmatrix} \alpha x_1 & \mathrm{x}_4 & \mathrm{x}_3 & (\alpha+1)x_2 \\ \mathrm{x}_1 & \mathrm{x}_4 & (\alpha+1)x_3 & \alpha x_2 \\ \mathrm{x}_1 & \mathrm{x}_4 & \alpha x_3 & \mathrm{x}_2 \\ (\alpha+1)x_1 & \alpha x_4 & \mathrm{x}_3 & \mathrm{x}_2 \end{bmatrix} | \forall x_1, x_2, x_3, x_4 \in F_{2^8} \right\}$$

Нехай $I \subseteq \{0,1,2,3\}$, де $0 < |I| < 4$,визначимо:

$$C_I = \bigoplus_{i \in I} C_i, D_I = \bigoplus_{i \in I} D_i, ID_I = \bigoplus_{i \in I} ID_i, M_I = \bigoplus_{i \in I} M_i.$$

Для наступних викладень, нагадамо, що ми використовуємо індекси I,$J \subseteq \{0,1,2,3\}$, котрі обчислюються за модулем 4.

Лема 1.1. $D_i \cap C_j = \langle e_{j-i,j} \rangle$, *та* $ID_i \cap C_j = \langle e_{j+i,j} \rangle$.

Лема 1.2. $C_i \cap M_j = \langle MC\langle e_{j-i,j} \rangle \rangle$.

Лема 1.3. $D_I \cap M_J\{0\}$, *та* $ID_I \cap M_J\{0\}$.

Опишемо деякі ланцюги підпросторів для одного раунду шифрування.

1) Нехай $I \subseteq \{0,1,2,3\}$, де $0 < |I| < 4$ та $a \in D_I^{\perp}$, тоді існує унікальне $b \in C_I^{\perp}$ таке, що $R_K(D_I \oplus a) = C_I \oplus b$.

2) Нехай $I \subseteq \{0,1,2,3\}$, де $0 < |I| < 4$ та $a \in C_I^{\perp}$, тоді існує унікальне $b \in M_I^{\perp}$ таке, що $R_K(C_I \oplus a) = M_I \oplus b$.

3) Якщо відкритий текст належав класу суміжності діагонального підпростору, то результат його шифрування буде належати класу суміжності змішаного підпростору. Зокрема, після 2-х раундів шифрування з фіксованим ключем отримаємо:

$$\Pr\left(R^{(2)}(u) \oplus R^{(2)}(v) \in M_i | u \oplus v \in D_I\right) = 1,$$

де $u \neq v$.

4) Якщо два відкритих тексти належать різним класам суміжності діагонального простору, то результат їх шифрування буде належати різним класам суміжності змішаного простору. Інакше:

$$\Pr\left(R^{(2)}(u) \oplus R^{(2)}(v) \in M_j | u \oplus v \in D_I\right) = 0,$$

де $u \neq v$.

5) З відкритого тексту, який належить класу суміжності діагонального простору, неможливо за два раунди шифрування одержати шифртекст із класу суміжності діагонального простору:

$$\Pr\left(R^{(2)}(u) \oplus R^{(2)}(v) \in D_j | u \oplus v \in D_I\right) = 0,$$

де $u \neq v$.

6) З відкритого тексту, який належить класу суміжності змішаного простору, неможливо за два раунди шифрування одержати шифртекст із класу суміжності змішаного простору:

$$\Pr\left(R^{(2)}(u) \oplus R^{(2)}(v) \in M_j | u \oplus v \in M_I\right) = 0,$$

де $u \neq v$.

Лема 1.4. *Для довільних M_I та C_J ми маємо:*

$$\Pr(x \in C_J | x \in M_I) = (2^8)^{-4|I|+|I||J}.$$

1.5 Модель розпізнавача із відомим ключем, що базується на властивостях ланцюгів підпросторів

Побудуємо модель розпізнавача із відомим ключем, що базується на властивостях ланцюгів підпросторів [7]. Задачею обох гравців є знаходження підпростору із 2^{64} пар відкритих текстів та шифртекстів (p^i,c^i), $i = 0,1,...2^{64}-1$, таких що для них виконуються наступні властивості [7]:

– для кожного $K \subseteq \{0,1,2,3\}$ з $\|K\| = 3$ відкриті тексти рівномірно розподілені та належать діагональному підпростору D_K

– для кожного $K \subseteq \{0,1,2,3\}$ з $\|K\| = 3$ шифртексти рівномірно розподілені та належать діагональному підпростору M_k

Якщо, фінальна *MixColumns* пропущена - еквівалентна умова на мові просторів: шифртекст котрий мав потрапити у M_k, потрапить у ID_k. В такому випадку, можливо переформулювати фінальну задачу для двох гравців можемо наступним чином: для (p^i,c^i), $i = 0,1,...2^{64}-1$ мають виконуються наступні властивості:

– для кожного $j,k = 0,1,2,3$ та для кожного $x \in F_{2^8}$ існує 2^{56} відкритих тексти $p^i, i \in I \subseteq \{0,..,2^{64}-1\}$, $\|I\| = 2^{32}$ що задовольняють умові ${p_{(j,k)}}^i = x, i \in I$

– для кожного $j,k = 0,1,2,3$ та для кожного $x \in F_{2^8}$ існує 2^{56} шифртексти $c^i, i \in I \subseteq \{0,..,2^{64}-1\}, \|I\| = 2^{32}$ що задовольняють умові ${c_{(j,k)}}^i = x, i \in I$

Зауважимо, ймовірність того, що рівномірний розподіл не збережеться на фінальному $MixColumns$, рівна нулю. Таким чином можна поставити наступну задачу гравцям: Знайти 2^{64} пар (p^i, c^i), $i = 0,..,2^{64} - 1$, таких що байти p^i та $MC^{-1}c^i$ рівномірно розподілені. Підкреслимо, що рівномірний розподіл полягає у збереженні властивості збалансованості для відкритих текстів та шифртекстів. Ймовірність збалансованності не руйнується фінальним $MixColumns$.

Переможна стратегія для чарівного гравця

Оберемо множину S, що складається з текстів, таких що: $S := D_i \oplus M_j \oplus c$, для певної константи c, де $\|S\| = 2^{64}$. Зауважимо, що:

$$D_i \oplus M_j \oplus c = \bigcup_{b \in D_i \oplus c} M_j \oplus b = \bigcup_{a \in M_j \oplus c} D_i \oplus a$$

Тобто, S може бути перевизначено, як об'єднання підпросторів D_i або об'єднання підпросторів M_j. Надалі, S подається як шифртекст отриманий після 4го раунду шифрування для дальнішого шифрування, та як відкритий текст 4го раунду для розшифрування (рис.1.2).

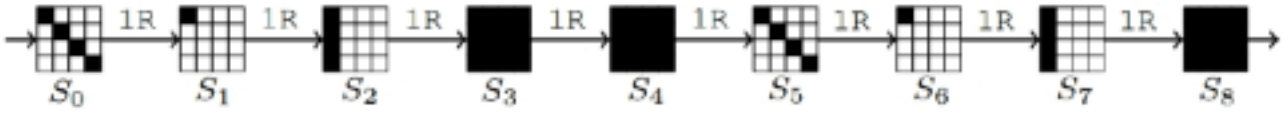

Рисунок 1.2 – Ланцюг підпросторів для чарівного гравця

Після зашифрування S після 4го раунду, текст буде залишатися рівномірно розподіленим для кожного підпростору M_I розмірнюстю 12 ($\|I\| = 3$). Таким чином, кожен підпростір M_I для $\|I\| = 3$ буде містити рівно 2^{32} елементи. Із властивостей зазначених раніше ми знаємо, що два елементи із одного підпростору D_I після 4х раундів шифрування не можуть потрапити до одного підпростору M_J для $\|I\| + \|J\| \leq 4$. Тобто, якщо ми візьмемо підпростір D_i з $\|i\| = 1$, то після 4х раундів шифрування всі елементи будуть розподілені по різним підпросторам $M_J, \|J\| = 3$. Оскільки підпростір D_i містить 2^{32} елементів та M_J також

містить рівно 2^{32} елементів, то ми можемо зробити висновок, що елементи з $D_i \oplus M_J$ рівномірно розподілені, для кожного M_I. Аналогічна властивість зберігається і при розшифруванні. Тому, після розшифрування S на 4 раунди також буде зберігатися рівномірний розподіл.

Алгоритм роботи чарівного гравця:

1) Генеруються 2^{64} елементів, що належать простору $S := D_i \oplus M_j \oplus c$, для певної константи c

2) Згенеровані елементи подаються як відкритий текст для зашифрування на 5-8 раунди. 2^{32} елементів будуть належати M_I.

3) Згенеровані елементи подаються як шифртекста для розшифрування на 3-1 раунди. 2^{32} елементів будуть належати D_I

4) Перевіряє чи зберігається рівномірний розподіл після шифрування/розшифрування.

При виконанні даного алгоритму, чарівний гравець завжди буде отримувати на виході рівномірно розподілені елементи для кожного з підпросторів.

В той час, звичайний гравець працює як чорний ящик. Ймовірність того, що 2^{64} текстів, згенеровані звичайним гравцем, будуть задовольняти рівномірному розподілу розраховується за наступною формулою:

$$p = \left(\prod_{i=0}^{255} C_{2^{64}-i2^{56}}^{2^{56}} (2^{-8})^{2^{64}} \right)^{16} \approx 2^{-7328,1}.$$

Розширена модель криптоаналізу із відомим ключем

У попередньому підрозділі було описано розпізнавач для 8ми раундів AES. Розширимо вже побудований сценарій для розпізновача до 10 раундів. Основна ідея полягає в наступному: Додамо один раунд на початку та у кінець шифрування. Нагадаємо – в даній роботі розглядається модифікована версія шифру – без фінального перетворення $MixColumns$. У сценарії розпізнавача із відомим ключем гравці мають

надіслати та верифікатору 2^{64} пар відкритих та шифр текстів, що задовольняють наступним властивостям:

– Існує ключ k^0 такий, що байти з $R_{k^0}(p^i)_i$ рівномірно розподілені над підпростором D_I для $\|I\| = 3$;

– Існує ключ k^{10} такий, що байти з $MC^{-1}({R_{k^{10}}}^{-1}(c^i)_i)$ рівномірно розподілені над підпростором M_J для $\|J\| = 3$;

В даній грі раундові ключі k^0 та k^{10} незалежні один від одного . Оскільки в даному сценарії використовіються тільки рівномірно розподілені текста, це передбачає виконання властивості збалансованості, тобто виконується наступна властивість: якщо для ключа k^0 сума відкритих текстів після першого раунду шифрування рівна 0, то для ключа k^{10} сума шифртекстів текстів перед останнім раундом шифрування, також, рівна 0.

Підкреслимо, що верифікатор має перевіряти попередню властивість без знання ключа. Верифікатор не має жодної інформації стосовно ключа, він має ефективно перевіряти виконання необхідної властивості. Таким чином, єдиний шлях для перевірки виконання вимог для k^0 та k^{10} верифікатором – це проведення повного їх перебору. Тобто, перевірити $2 * 2^{128} = 2^{129}$ можливих пар k^0 та k^{10}. Пропонується перевіряти рівномірний розподіл для одного стовпчика з $SR(c^i)$ та $SR^{-1}(p^i)$. У такому випадку – верифікатор має перевірити лише 32 байти з 128 – та повторити ще 4 рази (для кожної діагоналі та антидіагоналі) для кожного ключа.

Чарівний гравець має зконструювати 2^{64} пар відкритих та шифртекстів за тією самою стратегією, що і для 8 раундів. Ймовірність успіху в такому випадку для чарівного гравця рівна одиниці.

Доведено, що ймовірність того, що звичайний гравець згенерує пари, що задовольнять необхідним умовам складає $2^{-2^{12,81}}$. Надалі, верифікатор зможе знайти ключі k^0 та k^{10}, котрі задовольняють необхідним властивостям (якщо вони існують) зі складністю меншою ніж для двох гравців.

Висновки до розділу 1

У даному розділі було розглянуто новий метод побудови розпізнавача на відомих ключах, що використовує властивості ланцюгів підпросторів блокового шифру AES. Були введені поняття елементів, необхідних для побудови моделі, створені сценарії роботи елементів моделі. Оскільки блоковий шифр «Калина» має схожу на AES структуру, то надалі буде виконано спробу побудувати модель розпізнавача на відомих ключах з використанням властивостей ланцюгів підпросторів для «Калина»-подібних шифрів.

2 ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ «КАЛИНА»-ПОДІБНИХ ШИФРІВ ТА ПОБУДОВА МОДЕЛІ РОЗПІЗНАВАЧА НА ВІДОМИХ КЛЮЧАХ

Описану у попередньому розділі ідею побудови розпізнавача на відомих ключах, що використовує ланцюги підпросторів, буде застосовано до «Калина»-подібних шифрів.

2.1 Опис шифру «Калина»

Структура шифру «Калина» подібна до структури шифру $Rijndael$, але орієнтована на 64-бітні обчислювальні архітектури. Кількість раундів залежить від довжини відкритого тексту та довжини ключа. Відкритий текст подається у вигляді матриці розміром $a \times 8$, де $a \in \{2,4,8\}$. У даній роботі будемо розглядати випадок, коли $a = 8$. Базові перетворення для шифрування:

$$E_{l,k}^{K} = AddKey'^{K_t} \circ MixColumns \circ ShiftRows \circ SubBytes \circ \prod_{i=1}^{t-1} (AddKey^{K_i} \circ MixColumns \circ ShiftRows \circ SubBytes) \circ AddKey^{K_0},$$

де l – розмір внутрішнього стану блокового шифру (у бітах), K_i – раундовий ключ шифрування, k – довжина ключа шифрування (у бітах), $AddKey'^{K_i}$ – функція додавання циклового ключа K_i за модулем 2^{64}, $MixColumns(MC)$ – лінійне перетворення (множення матриці лінійного

перетворення на матрицю внутрішнього стану над скінченним полем), $ShiftRows(SR)$ – перестановка елементів $g_{i,j} \in GF(2^8)$ внутрішнього стану (циклічний зсув рядків вправо при матричному поданні), $SubBytes(S-box)$ – шар нелінійного бієктивного відображення, який виконує обробку векторів, заданих над V_8 (байтова підстановка), $AddKey^{K_i}$ – функція додавання циклового ключа K_i за модулем 2.

Позначимо через R одне раундове перетворення, тобто послідовне виконання процедур $SubBytes$, $ShiftRows$ та $MixColumns$, а також додавання із ключем. Через $R^{(i)}$ будемо позначати процедуру, яка складається з виконання послідовних i раундів (включно із додаванням проміжних раундових ключів).

Процедура $ShiftRows(SR)$ виконує циклічний зсув вправо рядків матриці стану $g_{i,j} \in GF(2^8)$. Кількість елементів зсуву залежить від номеру рядку $i \in \{0,1,\ldots,7\}$, розміру блоку $l \in \{128256, 512\}$, та обчислюється за формулою $\delta_i = \|\frac{i*l}{512}\|$.

Процедура $MixColumns()$ виконує множення кожного стовпчику матриці стану на спеціально підібрану матрицю. Кожен елемент $g_{i,j}$, матриці внутрішнього стану $G = (g_{i,j})$ розглядається як елемент скінченного поля $GF(2^8)$, яке утворене незвідним поліномом $\vartheta(x) = x^8 + x^4 + x^3 + x^2 + 1$. Відповідно, кожен елемент результуючої матриці стану $W = (w_{i,j})$ одержується як результат множення векторів довжини 8 над скінченним полем $GF(2^8)$ за формулою $w_{i,j} = v >>> i \otimes G_j$, де

$$v = (0x01, 0x01, 0x05, 0x01, 0x08, 0x06, 0x07, 0x04)$$

– вектор, що утворює циркулянтну матрицю МДР-коду і складається з послідовності байтових констант у шістнадцятковому поданні, які інтерпретуються як елементи поля $GF(2^8)$, при цьому циклічний зсув виконується відносно елементів вектора над скінченним полем.

Більш детальну інформацію про структуру та особливості блокового шифру ДСТУ 7624:2014 «Калина» можна одержати у [3].

2.2 Означення підпросторів та побудова ланцюгів підпросторів для «Калина»-подібних шифрів, з розміром блоку 512-біт

Введемо необхідні визначення для побудови ланцюгів підпросторів, та згадаємо вже побудовані нами раніше ланцюги підпросторів «Калина»-подібних шифрів [11].

Нехай F – раундова функція в ітеративному блоковому шифрі:

$$E_K(m) = k_n \oplus F(...F(k_1 \oplus F(k_0 \oplus m))),$$

де k_i – раундові ключі, отримані з основного ключа K за допомогою певного ключового розкладу. Вхідні повідомлення m розглядаються як бітові вектори із лінійного простору всіх бітових векторів відповідної довжини. Розглянемо пару підпросторів V_1 та V_2 таких, що для довільного вектору a існує унікальний вектор b (який залежить від a та ключа) такий, що повинне виконуватись співвідношення $F(V_1 \oplus a) \oplus K \subseteq V_2 \oplus b$, тобто F переводить кожен клас суміжності у якийсь інший клас суміжності.

Позначимо через $E = \{e_{0,0},\ldots,e_{8,8}\}$ – простір початкових станів шифру «Калина», де $e_{i,j}$ – окремі байти (8-бітові рядки). Визначимо чотири сімейства підпросторів E:

1) *Стовпчиковий простір* C_i визначимо як $C_i = \langle e_{0,i},e_{1,i},...,e_{7,i}\rangle$, $i \in \{0,\ldots,7\}$. Наприклад, C_0 для випадку $8 * 8$ буде мати вид, наведений на рис. 2.1:

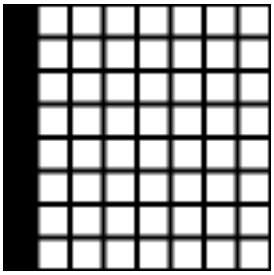

Рисунок 2.1 – Схематичний вид простору C_0 розміром $8 * 8$. Чорним позначено ненульові координати елементів простору.

2) *Діагональний простір* D_i визначимо як $D_i = SR^{-1}(C_i)$: $D_i = \langle e_{7,i}, e_{6,i+1}, ..., e_{0,i+7} \rangle$, де індекс $i + j$ обчислюється за модулем 8, $i \in \{0,\ldots,7\}$.Наприклад, D_0 для випадку $8 * 8$ буде мати вид, наведений на рис. 2.2:

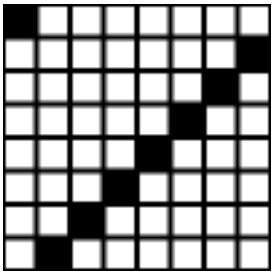

Рисунок 2.2 – Схематичний вид простору D_0 розміром $8 * 8$. Чорним позначено ненульові координати елементів простору.

3) *Інверсно-діагональний простір* ID_i визначимо як $ID_i = SR(C_i)$. $ID_i = \langle e_{0,i}, e_{1,i+1}, ..., e_{7,i+7} \rangle$, де індекс $i + j$ обчислюється за модулем 8, $i \in \{0,\ldots,7\}$.Наприклад, ID_0 для випадку $8 * 8$ буде мати вид, наведений на рис.2.3:

4) *Змішанний простір* M_i визначимо таким чином: $M_i = MC(ID_i)$.

Нехай $I \subseteq \{0,1,2,3,4,5,6,7\}$, де $0 < |I| < 8$,визначимо:

$$C_I = \bigoplus_{i \in I} C_i, D_I = \bigoplus_{i \in I} D_i, ID_I = \bigoplus_{i \in I} ID_i, M_I = \bigoplus_{i \in I} M_i.$$

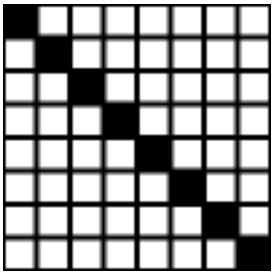

Рисунок 2.3 – Схематичний вид простору $\mathrm{I}D_0$ розміром $8 * 8$. Чорним позначено ненульові координати елементів простору.

Розмірність просторів и дорівнює $8*|I|$. Важливі підпростори в Калині побудовані з *діагональних просторів*, *інверсійно-діагональних просторів*, *стовпчикових просторів* та *змішанних*.

Визначення 2.1. *Ланцюгом підпросторів довжини* r назвемо простий кортеж з $r + 1$ підпросторів $(V_1,V_2,\ldots,V_{r+1})$, для яких виконуються співвідношення:

$$F(V_i \oplus a_i) \oplus K \subseteq V_{i+1} \oplus a_{i+1}.$$

Легко перевірити, що операція $SubBytes$ діагональні та стовпчикові простори переводить в діагоналні та стовпчикові(бієкція). Також, $ShiftRows$ діагональний простір переводить в стовпчиковий.

Надалі, при побудові ланцюгів підпросторів будуть використовуватися наступні властивості:

1) $D_i \cap C_j = \langle e_{j-i,j} \rangle$, та $ID_i \cap C_j = \langle e_{j+i,j} \rangle$.

2) $C_i \cap M_j = \langle MC\langle e_{j-i,j} \rangle \rangle$.

3) $D_I \cap M_J\{0\}$, та $ID_I \cap M_J\{0\}$.

Базуючись на вищезазначенних властивостях було побудовано наступні ланцюги підпросторів.

1) Нехай $I \subseteq \{0,1,...,7\}$, де $0 < |I| < 8$ та $a \in D_I^{\perp}$, тоді існує унікальне $b \in C_I^{\perp}$ таке, що $R_K(D_I \oplus a) = C_I \oplus b$, як це зображено на рис.2.4.

2) Нехай $I \subseteq \{0,1,...,7\}$, де $0 < |I| < 8$ та $a \in C_I^{\perp}$, тоді існує унікальне $b \in M_I^{\perp}$ таке, що $R_K(C_I \oplus a) = M_I \oplus b$.

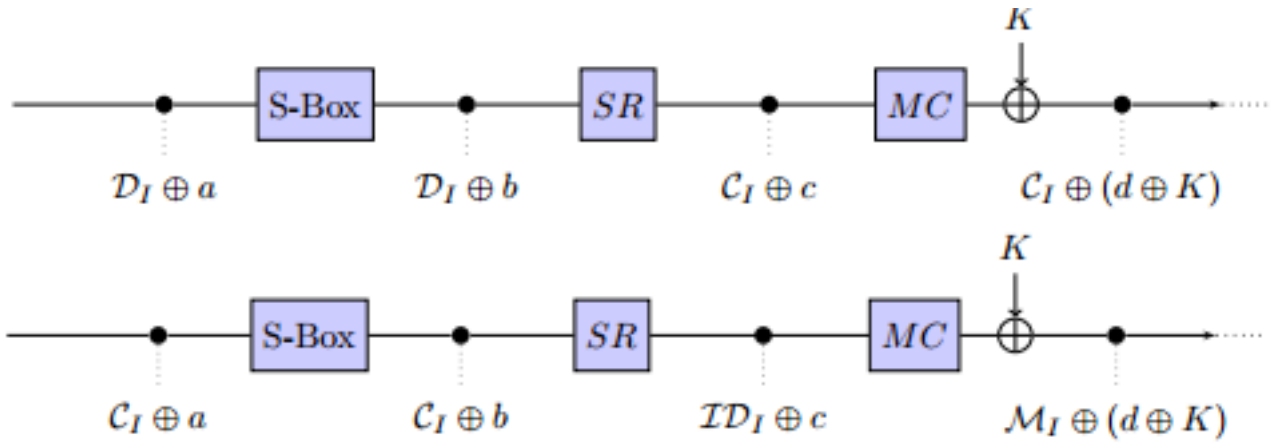

Рисунок 2.4 – Процес перетворення просторів для одного раунду

3) $\Pr\left(R^{(2)}(u) \oplus R^{(2)}(v) \in M_i | u \oplus v \in D_I\right) = 1$, де $u \neq v$.

4) $\Pr\left(R^{(2)}(u) \oplus R^{(2)}(v) \in M_j | u \oplus v \in D_I\right) = 0$, де $u \neq v$.

5) $\Pr\left(R^{(2)}(u) \oplus R^{(2)}(v) \in D_j | u \oplus v \in D_I\right) = 0$, де $u \neq v$.

6) $\Pr\left(R^{(2)}(u) \oplus R^{(2)}(v) \in M_j | u \oplus v \in M_I\right) = 0$, де $u \neq v$

7) Для довільних M_I та C_J виконується $\Pr(x \in C_J | x \in M_I) = (2^8)^{-8|I|+|I||J}$.

8) $\Pr\left(R^{(4)}(u) \oplus R^{(4)}(v) \in M_j | u \oplus v \in D_I\right) = 0$, де $u \neq v$.

Дані властивості використовуються як відмінна риса для криптоаналізу ітеративних блокових шифрів.

Візьмемо два відкритих тексти з D_I, з $I \subseteq \{0,1,2,3,4,5,6,7\}$, де $0 < |I| < 8$; з імовірністю 1 після двох раундів вони потраплять у підпростір M_I. Якщо замість «Калини» застосувати до цих текстів випадкову перестановку (ідеальний шифр), то ймовірність того, що вони потраплять в однаковий підпростір M_I дорівнює $(2^8)^{-64+8*|I|}$. Таким чином, достатньо однієї пари, щоб відрізнити випадкову перестановку від двох раундів шифрування «Калиною».

2.3 Перевірка необхідних властивостей для побудови моделі розпізнавача на відкритих ключах для «Калина»-подібних шифрів

Для успішної побудови моделі розпізнавача на відкритих ключах для ітеративного блокового шифру, необхідно перевірити наступні властивості:

1) Збереження властивості збалансованонності при зашифруванні. На скільки раундів шифрування розвовсюджується збереження властивості збалансованності?

2) Як пов'язані побудовані вище підпростори про рівномірному розподіленні байт і відкритому тексті?

Збереження збалансованності при зашифруванні

Перевіримо, чи зберігається властивість збалансованності при зашифруванні для «Калина»-подібних шифрів [12]. Для перевірки даної властивості для визначених раніше ланцюгів підпросторів при шифруванні та розшифруванні скористаємося основними властивостями інтегрального криптоаналізу. Введемо декілька означень:

– *Активні інтеграли* (A): це інтеграли, в котрих кожен елемент групи F_{2^8} повторюється однакову кількість разів в байті.

– *Константні інтеграли* (C): значення данного типа інтегралів зафіксоване для всіх текстів в байті.

– *Збалансовані* (B): XOR всіх значень у байті дорівнює 0.

Перевіримо, чи зберігається властивість збалансованності при побудові ланцюгів підпросторів.

1) Нехай на вхід шифрування подаються 2^{64} відкритих тексти, з однією активною діагоналлю (8 байт), всі інші байти константні. Побудуємо інтеграл для одного раунду шифрування (рис. 2.5): Тобто, на виході після одного раунду шифрування, ми отримаємо шифртексти з активним стовпчиком (8 байт), всі інші байти константні.

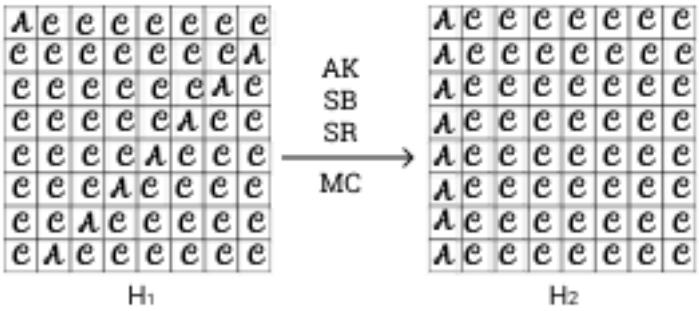

Рисунок 2.5 – Побудова інтегралу для відкритих текстів з однією активною діагоналлю

2) Нехай на вхід шифрування подаються 2^{64} відкритих тексти, з одним активним стовпчиком (8 байт), всі інші байти константні. Побудуємо інтеграл для одного раунду шифрування (рис. 2.6): Тобто, на

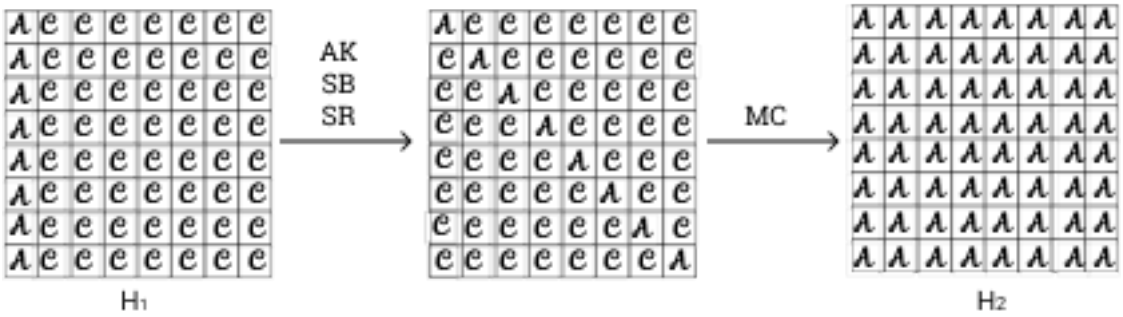

Рисунок 2.6 – Побудова інтегралу для відкритих текстів з одним активним стовпчиком

виході після одного раунду шифрування, ми отримаємо шифртексти з усіма активними байтами.

3) Нехай на вхід шифрування подаються 2^{64} відкритих тексти з усіма активними байтами. Побудуємо інтеграл для одного раунду шифрування (рис. 2.7): Тобто, на виході після одного раунду шифрування, ми отримаємо шифртексти з усіма збалансованими байтами.

Побудуємо композицію вищезазначених інтегралів. Нехай на вхід шифрування подаються 2^{64} відкритих тексти, з однією активною

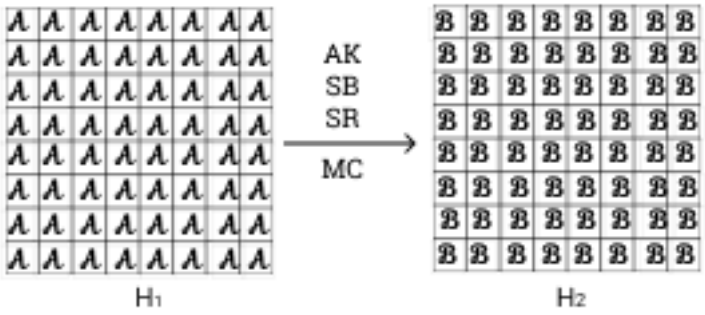

Рисунок 2.7 – Побудова інтегралу для відкритих текстів з усіма активними байтами

діагоналлю (8 байт), всі інші байти константні - тобто відкриті тексти, що належать діагональному підпростору. Тоді після трьох раундів шифрування ми отримаємо 2^{64} шифртексти з усіма активними байтами (властивість збалансованості зберігається). Після чотирьох раундів шифрування ми отримаємо 2^{64} шифртекстів, із збалансованими байтами (рис.). Аналогічні переходи справедливі і для розшифрування.

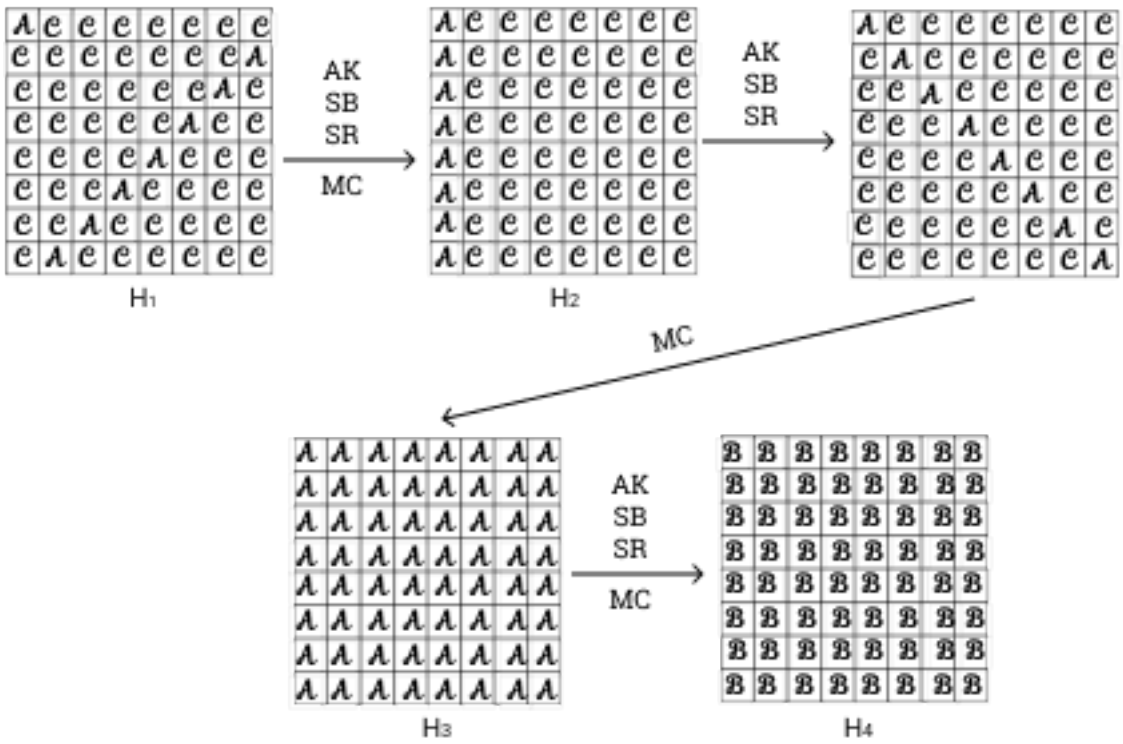

Рисунок 2.8 – Побудова інтегралу для відкритих текстів з усіма активними байтами

Отже, ми можемо зробити висновок, що при шифруванні до трьох раундів включно зберігається властивість збалансованості, якщо стартові відкриті тексти належать діагональному підпростору. Аналогічно, при шифруванні до двох раундів включно зберігається властивість збалансованості, якщо стартові відкриті тексти належать стовпчиковому підпростору, та на один раунд - якщо змішаному.

Взаємозв'язок між підпросторами з рівнорозподіленими байтами всередині

Перевіримо взаємоз'язок між зазначеними вище підпросторами при умові рівномірного розподілу байт всередині них.

Лема 2.1. *Нехай множина* $S = D_i \oplus M_j \oplus c$. *Тоді наступна властивість також справедлива для «Калина»-подібних шифрів:* $D_i \oplus M_j \oplus c = \bigcup_{b \in D_i \oplus c} M_j \oplus b = \bigcup_{a \in M_j \oplus c} D_i \oplus a$. *Тобто можина* S *може бути перевизначена як об'єднання підпросторів* D_i *або* M_i.

Доведення.

1) Нехай на вхід шифрування подаються 2^{64} відкритих текстів, що належать діагональному підпростору $D_i \oplus a$, $(a \in M_j)$. Тоді, після 2х раундів шифрування всі шифртексти будуть налележати змішанному підпростору M_J розмірності 56, тобто $R^{(2)}(D_i \oplus a) = M_J$. Раніше було доведено, що два елементи з одного підпростору D_I після шифрування не можуть потрапити у один і той самий підпростір з M_J, для $|I| + |J| \leqslant 8$. Візьмемо відкриті тексти, що належать підпростору та мають рівномірний розподіл всередині D_i для $|i| = 1$, тоді після 2го раунду всі елементи будуть розподілені по різним підпросторам M_J для $|J| = 7$. З цього випливає, що $D_i \oplus M_j = \bigcup_{a \in M_j} D_i \oplus a$. Тобто, якщо 2^{64} відкритих текстів належать підпростору $D_i \oplus M_j$ та є рівномірно розподіленими, то після двох раундів шифрування шифртексти будуть належати підпростору M_J та будуть залишатися рівномірно розподіленими.

2) Нехай 2^{64} шифртексти належать підпростору $M_j \oplus b$, $(b \in D_i)$ та є рівномірно розподіленими. Тоді після 2х раундів розшифрування отримані відкриті тексти будуть розподілені по різним підпросторам D_I

розмірності 56. З цього випливає, що $M_j \oplus D_i = \bigcup_{b \in D_i} M_j \oplus b$. Тобто, якщо 2^{64} шифртекстів належать підпростору $D_i \oplus M_j$ та є рівномірно розподіленими, то після двох раундів розшифрування відкриті тексти будуть належати підпростору D_I та будуть залишатися рівномірно розподіленими.

□

Отже, для «Калина»-подібних шифрів з розміром блоку 512 байтів при зашифруванні на 2 раунди зберігається умова збалансованності та рівномірна розподіленність текстів для запропонованих раніше ланцюгів підпросторів.

2.4 Побудова моделі розпізнавача на відкритих ключах для «Калина»-подібних шифрів

На основі отриманих результатів побудуємо модель розпізнавача з відомим ключем для «Калина»-подібних шифрів з розміром блоку 512 байтів. Введемо декілька означень:

Визначення 2.2. *T-складне відношення*: Нехай відображення $E : \{0,1\}^k * \{0,1\}^n \to \{0,1\}^n, (K,X) \to E_K(X)$ є блоковим шифром розміра n біт. Нехай $N \geqslant 1$ та R - натуральне число та довільне відношення над набором з S підпросторів по N елементів, що складаються з n-бітних блоків. Алгоритм A' конструює два підпростори, що складаються з N елементів $x' = (X'_i)$ та $y' = (Y'_i)$ такі що $Y'_i = \Pi(X'_i)$ та $x'Ry'$ із ймовірністю успіху $p \leqslant \frac{1}{2}$, де Π- випадково вибрана перестановка. Відношення R називається *T-складним відносно E*, якщо будь-який алгоритм A', виконується за час $T' \leqslant T$, де T'- дорівнює кількості обчислень над E.

Визначення 2.3. *Розпізнавач із відомим ключем*: Нехай відображення $E : \{0,1\}^k * \{0,1\}^n \to \{0,1\}^n, (K,X) \to E_K(X)$ є блоковим шифром розміра n біт. *Розпізнавачем із відомим ключем* назвемо пару (R,A) порядка $N \geqslant 1$, що складається з відношення R та алгоритма A. R - відношення над набором підпросторів по N елементів по n біт. Алгоритм A - на вході приймає k-бітний ключ K, за час T_A розраховує пару $x' = (X'_i)$ - над відкритим текстом та $y' = (Y'_i)$ над шифртекстом над E, такі що $Y'_i = E_K(X'_i)$, та обов'язково виконуються наступні умови:

1) Відношення R має бути T_A - складним по відношенню до E

2) Перевірка виконуваності відношення R має бути ефективно-перевіряємою - тобто не перевищувати T_A операцій.

Домовимося, що час необхідний для одного запиту до оракулу для отримання перестановки або її інверсії - рівний. Зауважимо, що для всіх ключів відповідність відношенню R має ефективно перевірятися без знання K.

Модель розпізнавача із відомим ключем для «Калина»-подібних шифрів із розміром блоку 512 байтів складається із наступних елементів: *генератор ключей, оракул, чарівний гравець, звичайний гравець, валідатор.*

– *Генератор* - генерує ключі шифрування

– *Чарівний гравець* - даний гравець знає ключ шифрування, працює за алгоритмом A та виконує роль "білого ящика".

– *Звичайний гравець* - даний гравець не знає ключа шифрування, для отримання шифртексту звертається до оракулу та виконує роль "чорного ящика". Оракул може генерувати шифртекст, використовуючи випадкову перестановку замість процесу шифрування.

– *Валідатор* - отримує дані від *чарівного та звичайного гравців.* Перевіряє, чи справді вони згенерували пари, для котрих виконується відношення R.

Для побудови сценарію роботи розпізнавача із відомим ключем важливо розуміти, якими метриками оцінюється успіх гравців. Можливі наступні способи:

1) Зафіксувати складність обчислень для кожного з гравців. В такому випадку, ми маємо оцінювати ймовірність перемоги гравців.

2) Для кожного з гравців зафіксувати ймовірність успіхів. В такому випадку, ми маємо оцінювати складність обчислень кожного з гравців, за якої він буде перемагати із фіксованую ймовірністю.

В даній роботі оцінювати успіх гравців будемо за допомогою розрахунку ймовірності перемоги гравців при умові однакової складності обчислень для кожного з гравців.

Сценарій роботи роботи розпізнавача складається з наступних кроків:

1) На старті обирається відношення R

2) Генератор ключей генерує ключ, котрий подається на вхід алгоритмів, котрі виконуються звичайним та чарівним гравцями.

3) Чарівний гравець та звичайний гравець генерують пари текстів заданого розміру, що відповідають відношенню R обраного на старті. Згенеровані тексти вони відправляють на перевірку валідатору.

4) Валідатор робить наступну перевірку: чи задовільняє згенерована пара відношенню R?
Зауважимо, що валідатор має ефективно робити перевірку.

5) Перемагає гравець, котрий генерує пари, що задовільняють відношенню R в більшою імовірністю.

Складність роботи розпізнавача - це сума складностей перевірок та конструювань пар відкритого тексту та шифртексту, котрі задовольняють заданим вимогам.

Трактування результатів роботи вищезазначеного сценарію: Можливі наступні фінали роботи вищезазначеного сценарію:

1) Перемагає звичайний гравець - у такому випадку ми можемо зробити висновок, що шифр не відрізняється від звичайної перестановки.

2) Перемагає чарівний гравець - у такому випадку ми можемо зробит висновок, що поведінку шифру у первих випадках ми можемо передбачити та підбирати вхідні дані спеціальним чином.

Оскільки успіх роботи звичайного гравця залежить від згенерованих оракулом даних, оцінювати складність його роботи ми можемо двома способами:

1) Складність обчислень для звичайного гравця визнається виключно кількістю звернень до оракулу.

2) Складність обчислень для звичайного гравця визначається, враховуючи кількість запитів гравця до оракулу та складність всіх інших обчислень гравця (у більшості випадків вона є незначною).

Оскільки у більшості випадків складність обчислень звичайного гравця добре апроксимується кількістю запитів до оракулу, то оцінювати складність обчислень ми будемо саме таким чином.

2.5 Модель розпізнавача із відомим ключем, що базується на властивостях ланцюгів підпросторів для 5 раундів для «Калина»-подібних шифрів із розміром блоку 512 бітів

Побудуємо модель криптоаналізу із відомим ключем для «Калина» подібних шифрів із розміром блоку 512 на основі вищеописанних властивостей спеціально підібраних підпросторів.

Зауважимо, що в даній моделі фінальна $AddKey$ пропущена.

Задачею обох гравців є знаходження підпростору, що складається із пар відкритих текстів та шифртекстів (p^i,c^i), для котрих виконуються наступні властивості:

– для кожного $K \subseteq \{0,1,2,3,4,5,6,7\}$ з $\|K\| = 7$ відкриті тексти рівномірно розподілені та належать діагональному підпростору D_K

– для кожного $K \subseteq \{0,1,2,3,4,5,6,7\}$ з $\|K\| = 7$ шифртексти рівномірно розподілені та належать змішаному підпростору M_k

Вже доведено, що після 2х раундів шифрування для рівномірно розподілених відкртих текстів, що належать діагональному підпростору зберігається рівномірний розподіл, а шифртексти належать змішаному підпростору.

Базуючись на даних властивостях ми можемо поставити наступну задачу гравцям: Знайти пари (p^i, c^i), такі що байти p^i та $MC^{-1}(c^i)$ були рівномірно розподілені.

За для того, щоб розширити кількість раундів з котрими працює розпізнавач скористаємося стратегією "Початок із середини". В даній роботі буде побудовано модель криптоаналізу із відкритим ключем для вибраних раундів. Побудуємо ланцюг підпросторів для «Калина»-подібних шифрів довжиною в 5 раундів за наступною стратегією:

1) На вхід 3го раунду шифрування подаються відкриті тексти що є рівномірно розподіленими та належать $D_i \oplus M_j$ підпростору.

2) Одночасно виконуємо розшифрування та зашифрування спеціальним чином підібраних текстів. Базуючись на властивостях ланцюгів підпросторів «Калина»-подібних шифрів, котрі були доведені вище, ми можемо побудувати наступний ланцюг переходів (рис. 2.9): $D_I \leftarrow C_i \leftarrow M_j \oplus D_i \rightarrow C_J \rightarrow M_J$.

Таким чином, на основі вже відомих нам властивостей ми побудували ланцюг підпросторів довжиною 5 раундів шифрування/розшифрування.

Отже, сформулюємо сценарій роботи розпізнавача, що базується на властивостях ланцюгів підпросторів для «Калина»-подібних шифрів.

Сценарій роботи розпізнавача, що базується на властивостях ланцюгів підпросторів

1) Оберемо відношення R наступним чином:

– в парі відкритий текст/шифртекст обидва елементи мають бути рівномірно розподіленими

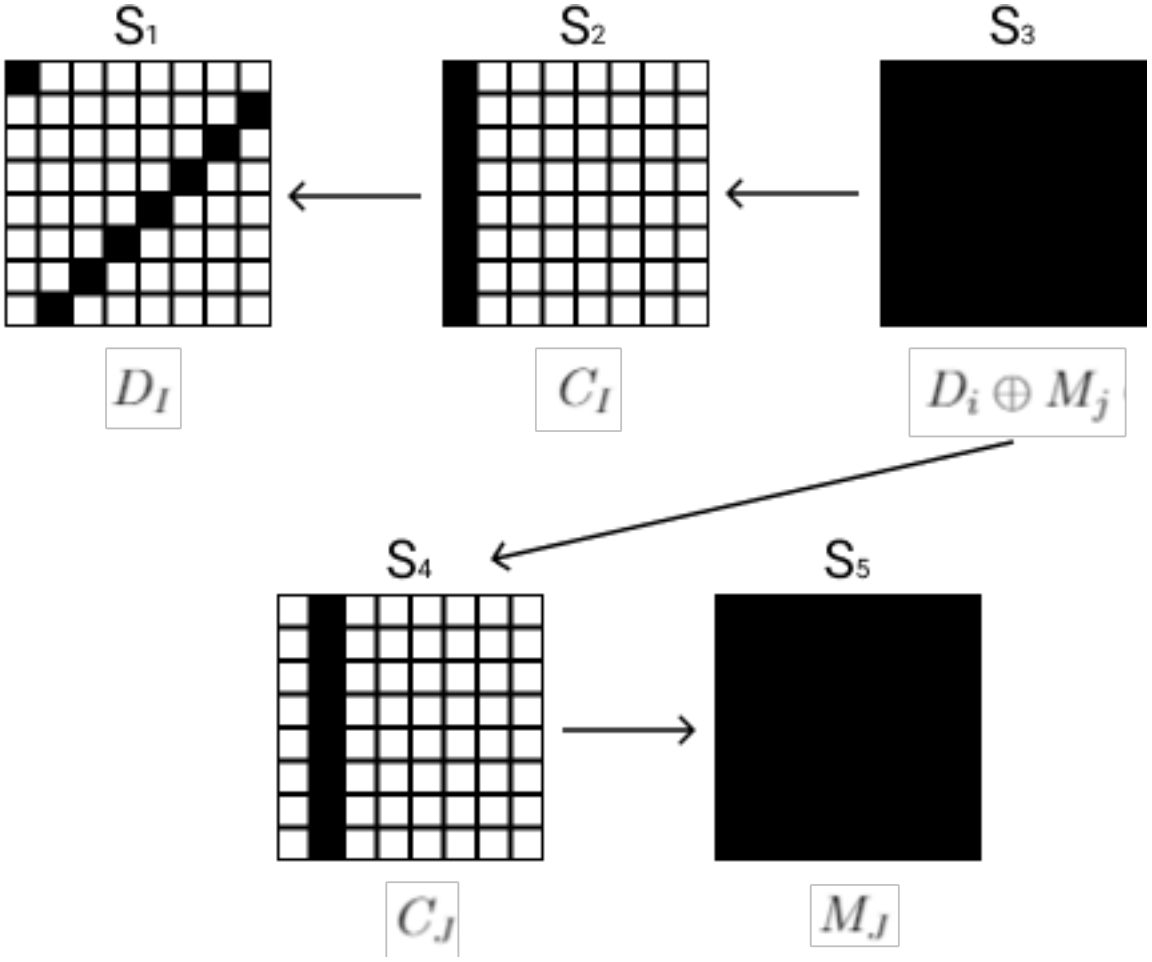

Рисунок 2.9 – Ланцюг підпросторів для 5 раундів для розпізнавача

– кожному відкритому тексту має відповідати правильний шифртекст, тобто для кожної пари (p_i, c_i) має виконуватися рівність $E_k(p_i)^{(2)} = c_i$ або $D_k(c_i)^{(2)} = p_i$

2) Генератор ключей генерує ключ, котрий подається на вхід алгоритмів, котрі виконуються звичайним та чарівним гравцями

3) Чарівний гравець та звичайний гравець генерують пари текстів заданого розміру, що є рівномірно розподіленими та для них виконується рівність $E_k(p_i)^{(2)} = c_i$ або $D_k(c_i)^{(2)} = p_i$

4) Згенеровані гравцями тексти вони відправляють на перевірку валідатору

5) Валідатор робить наступну перевірку: чи задовільняє згенерована пара відношенню R?

Зауважимо, що валідатор має ефективно робити перевірку.

6) Перемагає гравець, котрий генерує пари, що задовільняють відношенню R в більшою імовірністю

Алгоритм роботи та ймовірність перемоги для звичайного гравця

В даній моделі розпізнавача із відомим ключем звичайний гравець працює як «чорний ящик». При побудові моделі ми домовились, що оцінювати складність його роботи будемо ймовірністю перемоги кожного із гравців. Отже, розрахуємо ймовірність перемоги звичайного гравця.

Оскільки, фактично, успішність згенерованої пари звичайним гравцем залежить від того, чи буде зберігатися рівномірний розподіл для пари (p^i, c^i), розрахуємо ймовірність того, що оракул із рівномірно розподіленого на вході відкритого тексту, після застосування випадкової перестановки, згенерує рівномірно розподілений шифртекст на виході.

Дана ймовірність залежить від того, скільки байт буде зафіксовано при застосуванні до відкритого тексту випадкової перестановки.

Нехай t-кількість зафіксованих байт. Тоді ймовірність того що тексти, згенеровані звичайним гравцем, будуть задовольняти рівномірному розподілу розраховується за наступною формулою:

$$p = \left((\frac{(2^{8t})!}{(2^{8(t-1)})!^{2^8}})(\frac{1}{2^8})^{2^{8t}} \right)^{64}$$

Тоді, в залежності від того, яке значення буде приймати t, ми отримаємо наступні ймовірності успіху пари, згенерованої оракулом задовільнити відношення R.

Таблиця 2.1 – Ймовірність генерування оракулом пари шифртекста та відкритого текста в залежності від кількості зафіксованих байт

t	**Pr**	**t**	**Pr**	**t**	**Pr**	**t**	**Pr**
1	$2^{-14.3836}$	17	$2^{-20.0236}$	33	$2^{-21.009}$	49	$2^{-21.5891}$

Табл.2.1 – Продовження таблиці

t	Pr	t	Pr	t	Pr	t	Pr
2	$2^{-16.403}$	18	$2^{-20.1093}$	34	$2^{-21.053}$	50	$2^{-21.6187}$
3	$2^{-17.2131}$	19	$2^{-20.1903}$	35	$2^{-21.0956}$	51	$2^{-21.6476}$
4	$2^{-17.7288}$	20	$2^{-20.2669}$	36	$2^{-21.1371}$	52	$2^{-21.676}$
5	$2^{-18.1079}$	21	$2^{-20.3397}$	37	$2^{-21.1773}$	53	$2^{-21.7038}$
6	$2^{-18.4078}$	22	$2^{-20.409}$	38	$2^{-21.2165}$	54	$2^{-21.7312}$
7	$2^{-18.656}$	23	$2^{-20.4751}$	39	$2^{-21.2547}$	55	$2^{-21.758}$
8	$2^{-18.8677}$	24	$2^{-20.5383}$	40	$2^{-21.2918}$	56	$2^{-21.7843}$
9	$2^{-19.0522}$	25	$2^{-20.5989}$	41	$2^{-21.328}$	57	$2^{-21.8101}$
10	$2^{-19.2158}$	26	$2^{-20.657}$	42	$2^{-21.3634}$	58	$2^{-21.8355}$
11	$2^{-19.3628}$	27	$2^{-20.7128}$	43	$2^{-21.3979}$	59	$2^{-21.8605}$
12	$2^{-19.4961}$	28	$2^{-20.7666}$	44	$2^{-21.4316}$	60	$2^{-21.885}$
13	$2^{-19.6182}$	29	$2^{-20.8185}$	45	$2^{-21.4645}$	61	$2^{-21.9091}$
14	$2^{-19.7307}$	30	$2^{-20.8685}$	46	$2^{-21.4967}$	62	$2^{-21.9328}$
15	$2^{-19.8351}$	31	$2^{-20.9169}$	47	$2^{-21.5281}$	63	$2^{-21.9561}$
16	$2^{-19.9324}$	32	$2^{-20.9637}$	48	$2^{-21.559}$	64	$2^{-21.9791}$

Оскільки чарівний гравець, при генеруванні пар шифртексту та відкритого тексту використовує спеціальним чином підібрані підпростори, це означає що в його алгоритмі кількість активних байт, котрі будуть

змінюватися завжди буде кратна 8. За для того, зрівняти умови для чарівного та звичайного гравців, для звичайного гравця зафіксуємо $t = 16$. Тоді гравцям необхідно буде згенерувати 2^{128} пар відкритих ти шифртекстів. В такому випадку, ймовірність того, що звичайний гравець згенерує пари, що задовольняють відношенню R, буде дорівнювати $\approx 2^{-19,932}$.

Сформулюєио алгоритм роботи для звичайного гравця:

1) Оракул отримує від генератора ключ шифрування

2) Звичайний гравець отримує від оракулу пару (p^i, c^i), котрі мають задовільняти відношенню R, котре було визначени на старті

3) Звичайний гравець надсилає пару (p^i, c^i) валідатору

4) Звичайний гравець повторює попередні кроки 2^{128} разів.

Отже, головна мета звичайного гравця: згенерувати як умога більше пар відкритих за шифр текстів, котрі будуть задовільняти обране на старті відношення. За умови, що обидва гравці будуть генерувати 2^{128} пар, ймовірність для кожної пари, згеренованої звичайним гравцем задовільнити відношення R буде складати $\approx 2^{-19,932}$.

Переможна стратегія для чарівного гравця

Нехай множина S складається з текстів, таких що: $S := D_i \oplus M_j \oplus c$, для певної константи c. Зауважимо, що:

$$D_i \oplus M_j \oplus c = \bigcup_{b \in D_i \oplus c} M_j \oplus b = \bigcup_{a \in M_j \oplus c} D_i \oplus a$$

Тобто, S може бути перевизначена, як об'єднання підпросторів D_i або об'єднання підпросторів M_j. Надалі, S подається як відкритий текст для дальнішого шифрування на 4й та 5й раунди шифрування, та як шифртекст після 3го раунду для розшифрування.

Після зашифрування S на 4му та 5му раундах шифрування, текст буде залишатися рівномірно розподіленим для кожного підпростору M_I розмірнюстю 56 ($\|I\| = 7$). Таким чином, кожен підпростір M_I для $\|I\| = 3$ буде містити рівно 2^{64} елементи. Із властивостей зазначених

раніше ми знаємо, що два елементи із одного підпростору D_I після 2х раундів шифрування не можуть потрапити до одного підпростору M_J для $\|I\| + \|J\| \leq 7$. Тобто, якщо ми візьмемо підпростір D_i з $\|i\| = 1$, то після 2х раундів шифрування всі елементи будуть розподілені по різним підпросторам $M_J, \|J\| = 7$. Оскільки підпростір D_i містить 2^{64} елементів та M_J також містить рівно 2^{64} елементів, то ми можемо зробити висновок, що елементи з $D_i \oplus M_J$ рівномірно розподілені, для кожного M_I.

Аналогічна властивість зберігається і при розшифруванні. Тому, після розшифрування S на 2 раунди також буде зберігатися рівномірний розподіл.

Алгоритм роботи чарівного гравця:

1) Генеруються 2^{128} елементів, що належать простору $S := D_i \oplus M_j \oplus c$, для певної константи c

2) Згенеровані елементи подаються як відкритий текст для зашифрування на 4-5 раунди. 2^{64} елементів будуть належати M_I.

3) Згенеровані елементи подаються як шифртекст для розшифрування на 2-1 раунди. 2^{64} елементів будуть належати D_I

4) Перевіряє чи зберігається рівномірний розподіл після шифрування/розшифрування.

При виконанні даного алгоритму, чарівний гравець завжди буде отримувати на виході рівномірно розподілені елементи для кожного з підпросторів. Що було доведено раніше.

Результати роботи побудованого алгоритму

Отже, у побудованій моделі розпізнавача на відомих ключах для «Калина»-подібних шифрів завжди буде отримувати перемогу чарівний гравець - оскільки, якщо він буде генерувати відкриті тексти заданого типу, то завжди буде отримувати рівномірно разподілені шифр тексти. В свою чергу, ймовірність того, що звичайний гравець буде отримувати шифртексти із рівномірним розподілом значно менша.

Тобто, ми можемо зробити висновок, що «Калина»-подібні шифри за введених нами обмежень не ведуть себе як випадкова перестановка.

2.6 Розширена модель розпізнавача із відомим ключем, що базується на властивостях ланцюгів підпросторів для 5-ти раундів для «Калина»-подібних шифрів із розміром блоку 512 бітів

У попередньому підрозділі було описано розпізнавач, котрий працює на основі результатів від 5-ти раундів шифрування «Калина»-подібних шифрів. Розширимо вже побудований сценарій для розпізновача до 7 раундів.

Основна ідея полягає в наступному: Додамо один раунд на початкок та у кінець шифрування. У сценарії розпізнавача з відомим ключем гравці мають надіслати та верифікатору 2^{128} пар відкритих та шифр текстів, що задовольняють наступним властивостям:

– Існує ключ k^0 такий, що байти з $R_{k^0}(p^i)_i$, є рівномірно розподіленими над підпростором D_I для $\|I\| = 7$;

– Існує ключ k^7 такий, що байти з $MC^{-1}({R_{k^7}}^{-1}(c^i)_i)$, є рівномірно розподілені над підпростором M_J для $\|J\| = 7$;

В даному сценарії раундові ключі k^0 та k^7 незалежні один від одного.

Оскільки в даному сценарії використовіються тільки рівномірно розподілені текста, це передбачає виконання властивості збалансованості, тобто виконується наступна властивість: якщо для ключа k^0 сума відкритих текстів після першого раунду шифрування рівна 0, то для ключа k^{10} сума шифртекстів текстів перед останнім раундом шифрування, також, рівна 0. Раніше, нами вже було доведено збереження властивості збалансованності.

Підкреслимо, що верифікатор має перевіряти попередню властивість без знання ключа.

Верифікатор не має жодної інформації стосовно ключа, він має ефективно перевіряти виконання визначеної на старті властивості.

Таким чином, єдиний шлях для перевірки виконання вимог для k^0 та k^7 валідатором – це проведення повного їх перебору.

Тобто, валідатор має перевірити $2 * 2^{256} = 2^{257}$ можливих пар k^0 та k^7. За для того, щоб зменшити кількість перевірок, пропонується перевіряти рівномірний розподіл для одного стовпчика з $SR(c^i)$ та $SR^{-1}(p^i)$. У такому випадку – валідатор має перевірити лише 64 байти з 256 – та повторити ще 4 рази (для кожної діагоналі та антидіагоналі) для кожного ключа.

Отже, базуючись на попередніх викладках сформулюємо сценарій роботи розпізнавача.

Сценарій роботи розпізнавача для розширеної моделі:

1) Оберемо відношення R наступним чином:

– в парі відкритий текст/шифртекст обидва елементи мають бути рівномірно розподіленими

– кожному відкритому тексту має відповідати правильний шифртекст, тобто для кожної пари (p_i, c_i) має виконуватися рівність $E_k(p_i)^{(2)} = c_i$ або $D_k(c_i)^{(2)} = p_i$

2) Генератор ключей генерує ключ, котрий подається на вхід алгоритмів, котрі виконуються звичайним та чарівним гравцями

3) Чарівний гравець та звичайний гравець генерують 2^{128} пари текстів заданого розміру, що є рівномірно розподіленими та для них виконується рівність $E_k(p_i)^{(2)} = c_i$ або $D_k(c_i)^{(2)} = p_i$

4) Згенеровані гравцями тексти вони відправляють на перевірку валідатору

5) Валідатор робить виконує наступні кроки:

– Для всіх можливих значень k_0 та k_7 розшифровує та зашифровує отримані значення на 1 раунд

– В отриманих результатах для байтів, що знакодяться у одному стовпчику, діагоналі та антидіагоналі перевіряє чи є вони рівномірно розподіленими

– Підраховує кількість успіхів кожного з гравців

Зауважимо, що валідатор має ефективно робити перевірку.

6) Перемагає гравець, котрий генерує пари, що задовільняють відношенню R в більшою імовірністю

Чарівний гравець має зконструювати 2^{128} пар відкритих та шифртекстів за тією самою стратегією, що і для 5 раундів. Ймовірність успіху в такому випадку для чарівного гравця буде залишитися рівна одиниці.

Перевіримо ймовірність того, що після роботи валідатора згенерований звичайним гравцем шифртекст буде залишатися рівномірно розподіленим. Дана ймовірність залежить від того, скільки байт буде зафіксовано при застосуванні до відкритого тексту випадкової перестановки.

Нехай t-кількість зафіксованих байт. Тоді ймовірність того що тексти, згенеровані звичайним гравцем під час роботи валідатора, будуть задовольняти рівномірному розподілу розраховується за наступною формулою:

$$p = \left((\frac{(2^{8t})!}{(2^{8(t-1)})!^{2^8}})(\frac{1}{2^8})^{2^{8t}} \right)^{64} * 2^{512}$$

Тоді, в залежності від того, яке значення буде приймати t, ми отримаємо наступні ймовірності успіху пари, згенерованої оракулом задовільнити відношення R.

Таблиця 2.2 – Ймовірність генерування оракулом пари шифртекста та відкритого текста в залежності від кількості зафіксованих байт

t	**Pr**	**t**	**Pr**	**t**	**Pr**	**t**	**Pr**
1	$2^{-14.3486}$	17	$2^{-20.0229}$	33	$2^{-21.0087}$	49	$2^{-21.5889}$
2	$2^{-16.3944}$	18	$2^{-20.1087}$	34	$2^{-21.0527}$	50	$2^{-21.6184}$

Табл.2.2 – Продовження таблиці

t	Pr	t	Pr	t	Pr	t	Pr
3	$2^{-17.2082}$	19	$2^{-20.1897}$	35	$2^{-21.0953}$	51	$2^{-21.6474}$
4	$2^{-17.7254}$	20	$2^{-20.2663}$	36	$2^{-21.1367}$	52	$2^{-21.6758}$
5	$2^{-18.1052}$	21	$2^{-20.3392}$	37	$2^{-21.177}$	53	$2^{-21.7036}$
6	$2^{-18.4057}$	22	$2^{-20.4085}$	38	$2^{-21.2162}$	54	$2^{-21.7309}$
7	$2^{-18.6542}$	23	$2^{-20.4746}$	39	$2^{-21.2544}$	55	$2^{-21.7578}$
8	$2^{-18.8661}$	24	$2^{-20.5378}$	40	$2^{-21.2915}$	56	$2^{-21.7841}$
9	$2^{-19.0509}$	25	$2^{-20.5984}$	41	$2^{-21.3278}$	57	$2^{-21.8099}$
10	$2^{-19.2146}$	26	$2^{-20.6565}$	42	$2^{-21.3631}$	58	$2^{-21.8353}$
11	$2^{-19.3617}$	27	$2^{-20.7124}$	43	$2^{-21.3976}$	59	$2^{-21.8603}$
12	$2^{-19.4951}$	28	$2^{-20.7662}$	44	$2^{-21.4313}$	60	$2^{-21.8848}$
13	$2^{-19.6172}$	29	$2^{-20.8181}$	45	$2^{-21.4642}$	61	$2^{-21.9089}$
14	$2^{-19.7298}$	30	$2^{-20.8681}$	46	$2^{-21.4964}$	62	$2^{-21.9326}$
15	$2^{-19.8343}$	31	$2^{-20.9165}$	47	$2^{-21.5279}$	63	$2^{-21.956}$
16	$2^{-19.9317}$	32	$2^{-20.9633}$	48	$2^{-21.5587}$	64	$2^{-21.9789}$

Оскільки чарівний гравець, при генеруванні пар шифртексту та відкритого тексту використовує спеціальним чином підібрані підпростори, це означає що в його алгоритмі кількість активних байт, котрі будуть змінюватися завжди буде кратна 8. За для того, зрівняти умови для

чарівного та звичайного гравців, для звичайного гравця зафіксуємо $t = 16$. Тоді гравцям необхідно буде згенерувати 2^{128} пар відкритих ти шифртекстів. В такому випадку,ймовірність того, що звичайний гравець згенерує пари, що задовольняють відношення R буде дорівнювати $\approx 2^{-19,931}$.

В побудованій розширеній моделі розпізнавача із відомим ключем алгоритми роботи чарівного та звичайного гравців залишаються незмінними. Змінюється лише алгоритм роботи валідатора.

Результати роботи побудованого алгоритму

Отже, в побудованому сценарії завжди буде перемагати чарівний гравець. Доведено, що ймовірність того, що звичайний гравець згенерує пари, що задовольнять необхідним умовам складає $2^{-2^{19,931}}$ за умови, що він буде генерувати 2^{128} шифртекстів із фіксованими 16 байтами.

Оскільки у побудованому сценарії перемогу завжди будет отримувати чарівний гравець, це говорить про те, що за заданих нами обмежень «Калина»-подібні шифри відрізняються від випадкової перестановки. Але, важливо зазначити, що для коректної роботи побудована модель потребує багато ресурсів часу та пам'яті. Тому, знайдена вразливість, на сьогодні не є критичною.

2.7 Модель розпізнавача із відомим ключем, що базується на властивостях ланцюгів підпросторів для 7 раундів для «Калина»-подібних шифрів із розміром блоку 512

Побудуємо модель розпізнавача із відомим ключем для «Калина»-подібних шифрів із розміром блоку 512 біт на основі властивостей спеціально підібраних підпросторів для 7 раундів шифрування.

Зауважимо, що в даній моделі фінальна $AddKey$ пропущена.

Задачею обох гравців є знаходження підпростору, що складається із пар відкритих текстів та шифртекстів (p^i,c^i), для котрих виконуються наступні властивості:

– для кожного $K \subseteq \{0,1,2,3,4,5,6,7\}$ з $\|K\| = 7$ відкриті тексти рівномірно розподілені та належать діагональному підпростору D_K

– для кожного $K \subseteq \{0,1,2,3,4,5,6,7\}$ з $\|K\| = 7$ шифртексти рівномірно розподілені та належать змішаному підпростору M_k

Вже доведено, що після 2х раундів шифрування для рівномірно розподілених відкртих текстів, що належать діагональному підпростору зберігається рівномірний розподіл, а шифртексти належать змішаному підпростору.

Розглянемо частковий випадок, при побудові ланцюгів підпросторів, а саме можливі переходи після шифрування текстів, що належать діагональному підпростору.

Нехай, на вхід шифрування подається елемент із однією активною діагоналлю (8 активних байт). Нехай даний елемент належить підпростору D_I. Тоді, із ймовірністю $\frac{1}{2^{56}}$ після одного раунду шифрування отриманий шифртекст буде належати стовпчиковому підпростору C_I але тільки з одним активним елементом. Тобто отриманий ланцюг виглядає наступним чином (рис. 2.10):

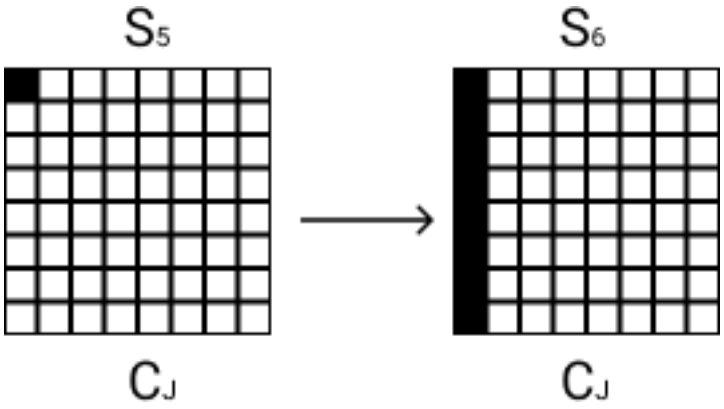

Рисунок 2.10 – Частковий випадок переходу із діагонального підпростору у стовпчиковий із одним активним байтом

Таким чином, ми можемо побудувати ймовірнісний ланцюг підпросторів довжиною в 4 раунди, а саме (рис. 2.11):

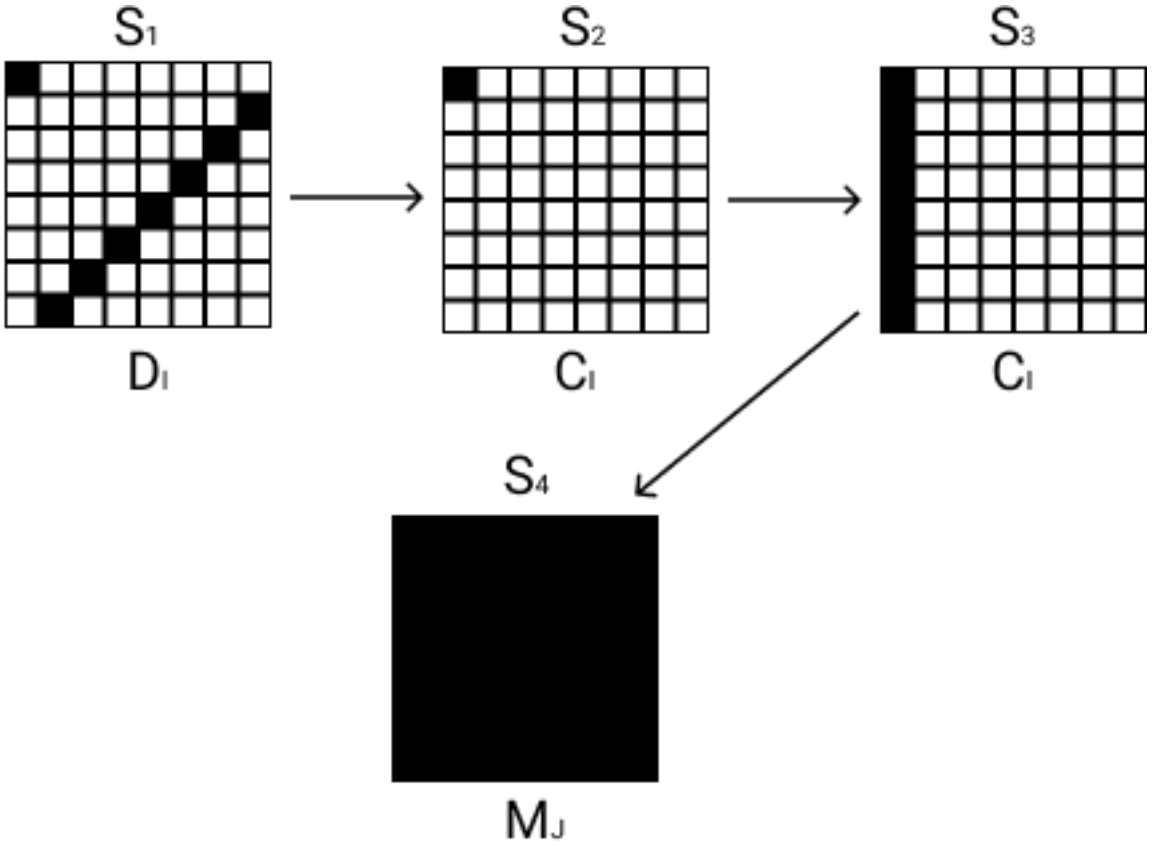

Рисунок 2.11 – Ймовірнісний ланцюг підпросторів довжиной 4 раунди

Перевіримо, чи зберігається властивість збалансованості при побудові ймовірнісного ланцюга.

Нехай на вхід шифрування подаються 2^{64} відкритих тексти, з однією активною діагоналлю (8 байт), всі інші байти константні. Побудуємо інтеграл, що є частковим випадком для одного раунду шифрування (рис. 2.12):

Тобто, на виході після одного раунду шифрування, ми отримаємо шифртексти з активним стовпчиком (1 байт), всі інші байти константні.

Побудуємо композицію вже побудованих раніше інтегралів та інтегралу, що є частковим випадком для одного раунду шифрування.

Нехай на вхід шифрування подаються 2^{64} відкритих тексти, з однією активною діагоналлю (8 байт), всі інші байти константні - тобто відкриті

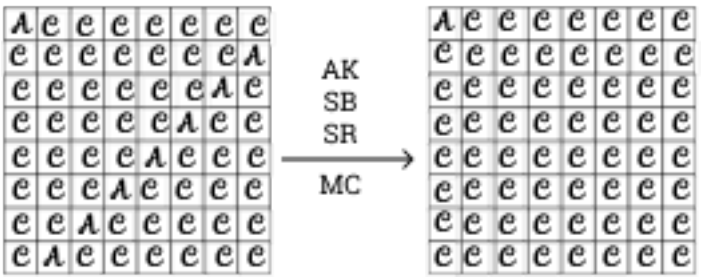

Рисунок 2.12 – Побудова часткового випадку інтегралу для відкритих текстів з однією активною діагоналлю

тексти, що належать діагональному підпростору. Тоді після чотирьох раундів шифрування, із ймовірністю $\frac{1}{2^{56}}$, ми отримаємо 2^{64} шифртексти з усіма активними байтами (властивість збалансованості зберігається).

Після п'яти раундів шифрування ми отримаємо 2^{64} шифртекстів, із збалансованими байтами (рис.2.13).

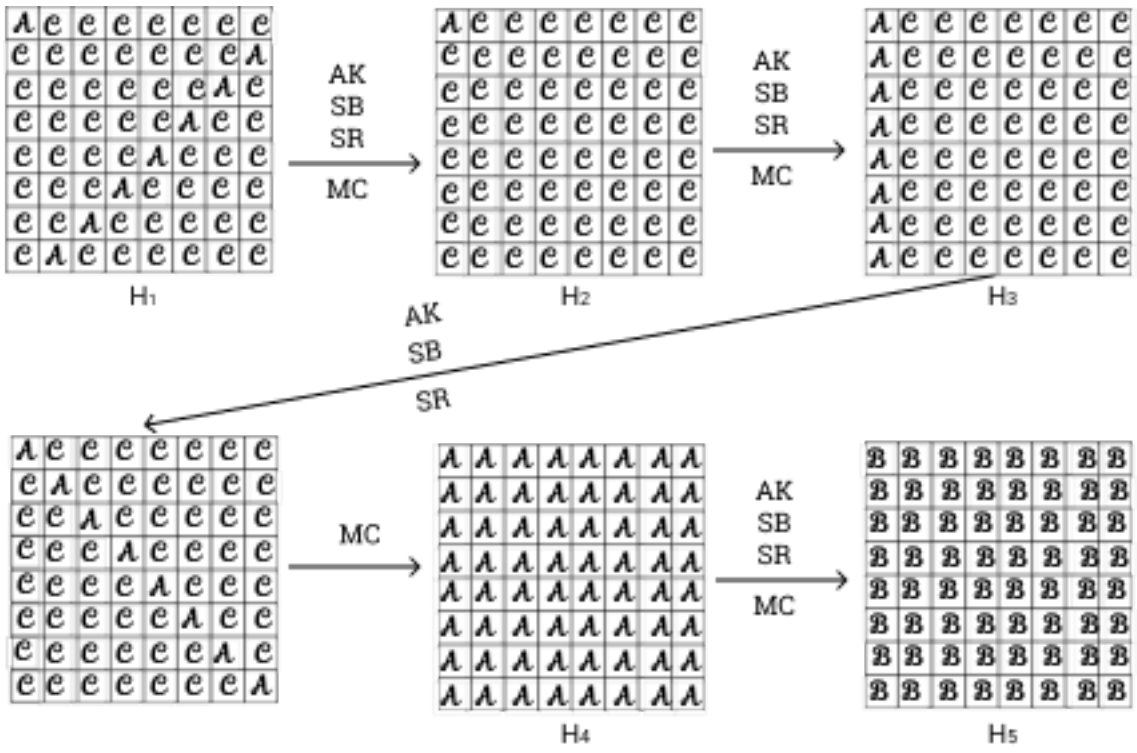

Рисунок 2.13 – Побудова часткового випадку інтегралу для 5 раундів шифрування

Аналогічні переходи справедливі і для розшифрування.

Отже, ми можемо зробити висновок, що при зашифруванні/розшифруванні вищезазначеного часткового випадку, властивість збалансованості зберігається до 5 раундів шифрування.

За для того, щоб розширити кількість раундів з котрими працює розпізнавач, скористаємося стратегією "Початок із середини". В даній роботі буде побудовано модель розпізнавача із відкритим ключем для вибраних раундів. Важливо зазначити, що в даній моделі всі ключі шифрування незалежні один від одного.

Побудуємо ланцюг підпросторів для «Калина»-подібних шифрів довжиною в 7 раундів за наступною стратегією:

1) На вхід 4го раунду шифрування подаються відкриті тексти що є рівномірно розподіленими та належать $D_i \oplus M_j$ підпростору.

2) Одночасно виконуємо розшифрування та зашифрування спеціальним чином підібраних текстів. Базуючись на властивостях ланцюгів підпросторів «Калина»-подібних шифрів, котрі були доведені вище, ми можемо побудувати наступний ланцюг переходів (рис. 2.14):

Таким чином, на основі вже відомих нам властивостай ми побудували ланцюг підпросторів довжиною 7 раундів шифрування/розшифрування.

Базуючись на вищезазначених властивостях ланцюгів підпросторів для 7 раундів шифрування «Калина»-подібних шифрів, сформулюємо сценарій роботи для розпізнавача на відомих ключах.

Сценарій роботи розпізнавача, що базується на властивостях ланцюгів підпросторів для 7 раундів шифрування

1) Оберемо відношення R наступним чином:

– в парі відкритий текст/шифртекст обидва елементи мають бути рівномірно розподіленими

– кожному відкритому тексту має відповідати правильний шифртекст, тобто для кожної пари (p_i, c_i) має виконуватися рівність $E_k(p_i)^{(3)} = c_i$ або $D_k(c_i)^{(3)} = p_i$ із ймовірністю $\frac{1}{2^{56}}$.

2) Генератор ключей генерує ключ, котрий подається на вхід алгоритмів, котрі виконуються звичайним та чарівним гравцями

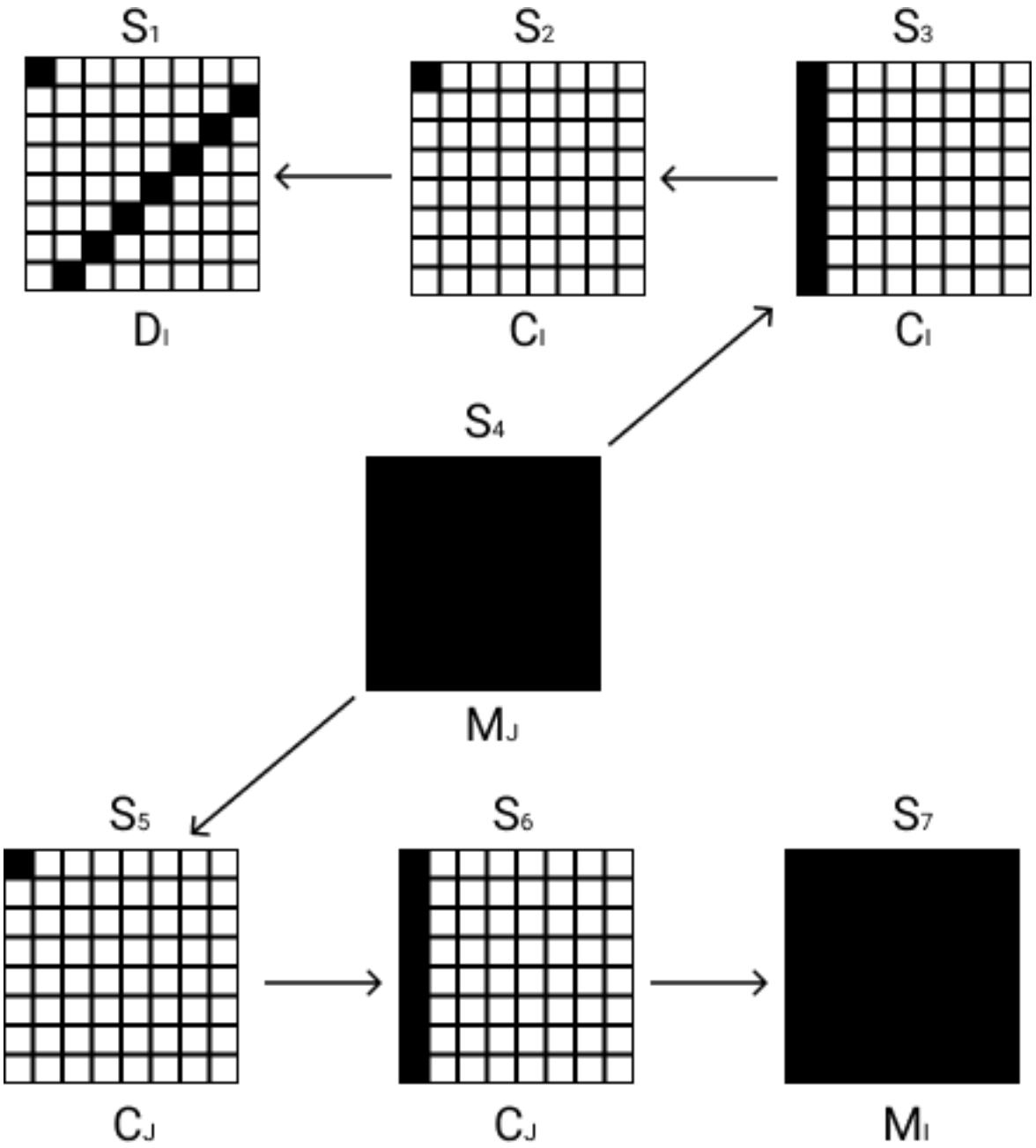

Рисунок 2.14 – Ланцюг підпросторів для 7 раундів шифрування

3) Чарівний гравець та звичайний гравець генерують пари текстів заданого розміру, що є рівномірно розподіленими.

4) Згенеровані гравцями тексти вони відправляють на перевірку валідатору

5) Валідатор робить наступну перевірку: чи задовільняє згенерована пара відношенню R?

Зауважимо, що валідатор має ефективно робити перевірку.

6) Перемагає гравець, котрий генерує пари, що задовільняють відношенню R в більшою імовірністю

Алгоритм роботи та ймовірність перемоги для звичайного гравця

В даній моделі розпізнавача із відомим ключем звичайний гравець працює як «чорний ящик». При побудові моделі ми домовились, що оцінювати складність його роботи будемо ймовірністю перемоги кожного із гравців. Отже, розрахуємо ймовірність перемоги звичайного гравця.

Оскільки, фактично, успішність згенерованої пари звичайним гравцем залежить від того, чи буде зберігатися рівномірний розподіл для пари (p^i, c^i), розрахуємо ймовірність того, що оракул із рівномірно розподіленого на вході відкритого тексту, після застосування випадкової перестановки, згенерує рівномірно розподілений шифртекст на виході.

Дана ймовірність залежить від того, скільки байт буде зафіксовано при застосуванні до відкритого тексту випадкової перестановки.

Нехай t-кількість зафіксованих байт. Тоді ймовірність того що тексти, згенеровані звичайним гравцем, будуть задовольняти рівномірному розподілу розраховується за наступною формулою:

$$p = \left((\frac{(2^{8t})!}{(2^{8(t-1)})!^{2^8}})(\frac{1}{2^8})^{2^{8t}} \right)^{64}$$

Тоді, в залежності від того, яке значення буде приймати t, ми отримаємо наступні ймовірності успіху пари, згенерованої оракулом задовільнити відношення R.

Таблиця 2.3 – Ймовірність генерування оракулом пари шифртекста та відкритого текста в залежності від кількості зафіксованих байт

t	**Pr**	**t**	**Pr**	**t**	**Pr**	**t**	**Pr**
1	$2^{-14.3836}$	17	$2^{-20.0236}$	33	$2^{-21.009}$	49	$2^{-21.5891}$

Табл.2.3 – Продовження таблиці

t	Pr	t	Pr	t	Pr	t	Pr
2	$2^{-16.403}$	18	$2^{-20.1093}$	34	$2^{-21.053}$	50	$2^{-21.6187}$
3	$2^{-17.2131}$	19	$2^{-20.1903}$	35	$2^{-21.0956}$	51	$2^{-21.6476}$
4	$2^{-17.7288}$	20	$2^{-20.2669}$	36	$2^{-21.1371}$	52	$2^{-21.676}$
5	$2^{-18.1079}$	21	$2^{-20.3397}$	37	$2^{-21.1773}$	53	$2^{-21.7038}$
6	$2^{-18.4078}$	22	$2^{-20.409}$	38	$2^{-21.2165}$	54	$2^{-21.7312}$
7	$2^{-18.656}$	23	$2^{-20.4751}$	39	$2^{-21.2547}$	55	$2^{-21.758}$
8	$2^{-18.8677}$	24	$2^{-20.5383}$	40	$2^{-21.2918}$	56	$2^{-21.7843}$
9	$2^{-19.0522}$	25	$2^{-20.5989}$	41	$2^{-21.328}$	57	$2^{-21.8101}$
10	$2^{-19.2158}$	26	$2^{-20.657}$	42	$2^{-21.3634}$	58	$2^{-21.8355}$
11	$2^{-19.3628}$	27	$2^{-20.7128}$	43	$2^{-21.3979}$	59	$2^{-21.8605}$
12	$2^{-19.4961}$	28	$2^{-20.7666}$	44	$2^{-21.4316}$	60	$2^{-21.885}$
13	$2^{-19.6182}$	29	$2^{-20.8185}$	45	$2^{-21.4645}$	61	$2^{-21.9091}$
14	$2^{-19.7307}$	30	$2^{-20.8685}$	46	$2^{-21.4967}$	62	$2^{-21.9328}$
15	$2^{-19.8351}$	31	$2^{-20.9169}$	47	$2^{-21.5281}$	63	$2^{-21.9561}$
16	$2^{-19.9324}$	32	$2^{-20.9637}$	48	$2^{-21.559}$	64	$2^{-21.9791}$

Оскільки чарівний гравець, при генеруванні пар шифртексту та відкритого тексту використовує спеціальним чином підібрані підпростори, це означає що в його алгоритмі кількість активних байт, котрі будуть

змінюватися завжди буде кратна 8. За для того, зрівняти умови для чарівного та звичайного гравців, для звичайного гравця зафіксуємо $t = 16$. Тоді гравцям необхідно буде згенерувати 2^{128} пар відкритих ти шифртекстів. В такому випадку,ймовірність того, що звичайний гравець згенерує пари, що задовольняють відношення R буде дорівнювати $\approx 2^{-19,932}$.

Сформулюємо алгоритм роботи для звичайного гравця:

1) Оракул отримує від генератора ключ шифрування

2) Звичайний гравець отримує від оракулу пару (p^i, c^i), котрі мають задовільняти відношенню R, котре було визначени на старті

3) Звичайний гравець надсилає пару (p^i, c^i) валідатору

4) Звичайний гравець повторює попередні кроки 2^{128} разів.

Отже, головна мета звичайного гравця: згенерувати як умога більше пар відкритих за шифр текстів, котрі будуть задовільняти обране на старті відношення. За умови, що обидва гравці будуть генерувати 2^{128} пар, ймовірність для кожної пари, згеренованої звичайним гравцем задовільнити відношення R буде складати $\approx 2^{-19,932}$.

Переможна стратегія для чарівного гравця

Нехай множина S складається з текстів, таких що: $S := D_i \oplus M_j \oplus c$, для певної константи c. Зауважимо, що:

$$D_i \oplus M_j \oplus c = \bigcup_{b \in D_i \oplus c} M_j \oplus b = \bigcup_{a \in M_j \oplus c} D_i \oplus a$$

Тобто, S може бути перевизначена, як об'єднання підпросторів D_i або об'єднання підпросторів M_j.

Надалі, S подається як відкритий текст для дальнішого шифрування на 4й -6й раунди шифрування, та як шифртекст після 4го раунду для розшифрування.

Зауважимо, на відміну від моделі розпізнавача із відомим ключем для 5 раундів, побудованої вище, дана модель є ймовірнісною, оскільки ймовірність переходу від простору $D_I \rightarrow C_i$ із одним активним байтом

при зашифруванні, та переходу C_I (із 8 активними байтами) $\rightarrow$ C_i із одним активним байтом при розшифруванні складає $\frac{1}{2^{56}}$.

Після зашифрування S на 4му, 5му та 6му раундах шифрування, текст буде залишатися рівномірно розподіленим для кожного підпростору M_I розмірнюстю 56 ($\|I\| = 7$).

Таким чином, кожен підпростір M_I для $\|I\| = 7$ буде містити рівно 2^{64} елементи. Із властивостей зазначених раніше ми знаємо, що два елементи із одного підпростору D_I після 3х раундів шифрування не можуть потрапити до одного підпростору M_J для $\|I\| + \|J\| \leq 7$. Тобто, якщо ми візьмемо підпростір D_i з $\|i\| = 1$, з ймовірністю $\frac{1}{2^{56}}$, то після 3х раундів шифрування всі елементи будуть розподілені по різним підпросторам $M_J, \|J\| = 7$. Оскільки підпростір D_i містить 2^{64} елементів та M_J також містить рівно 2^{64} елементів, то ми можемо зробити висновок, що елементи з $D_i \oplus M_J$ рівномірно розподілені, для кожного M_I.

Аналогічна властивість зберігається і при розшифруванні. Тому, після розшифрування S на 2 раунди також буде зберігатися рівномірний розподіл.

Алгоритм роботи чарівного гравця:

1) Генеруються 2^{128} елементів, що належать простору $S := D_i \oplus M_j \oplus c$, для певної константи c

2) Згенеровані елементи подаються як відкритий текст для зашифрування на 4-6 раунди. 2^{64} елементів будуть належати M_I з ймовірністю $\frac{1}{2^{56}}$.

3) Згенеровані елементи подаються як шифртекст для розшифрування на 3-1 раунди. 2^{64} елементів будуть належати D_I з ймовірністю $\frac{1}{2^{56}}$.

4) Перевіряє чи зберігається рівномірний розподіл після шифрування/розшифрування.

При виконанні даного алгоритму, чарівний гравець з ймовірністю $\frac{1}{2^{112}}$ буде отримувати на виході рівномірно розподілені елементи для кожного з підпросторів. Що було доведено раніше.

Результати роботи побудованого алгоритму

Отже, у побудованій моделі розпізнавача на відомих ключах дла «Калина»-подібних шифрів завжди буде отримувати перемогу чарівний гравець - оскільки, якщо він буде генерувати відкриті тексти заданого типу, то з ймовірністю $\frac{1}{2^{112}}$ буде отримувати рівномірно разподілені шифр тексти. В свою чергу, ймовірність того, що звичайний гравець буде отримувати шифртексти із рівномірним розподілом значно менша. Тобто, ми можемо зробити висновок, що «Калина»-подібні шифри за введених нами обмежень не ведуть себе як випадкова перестановка. Але, слід зазначити, що для практичної реалізації даної моделі необхідно необхідно провести щонайменще 2^{130} операцій. Тобто, дана модель дозволяє довести відмінність шифру від звичайної перестановки, але не за поліноміальний час. Саме тому, знайдена вразливість, не є критичною на сьогодні.

Висновки до розділу 2

В результаті проведеної роботи було виконано поставлену задачу, а саме: побудовано модель розпізнавача на відомих ключах, що використовує властивості ланцюгів підпросторів для «Калина»-подібних шифрів. В результаті побудови даної моделі було виявлено, що що «Калина»-подібні шифри за введених нами обмежень не ведуть себе як випадкова перестановка. Це означає, що зловмисник може скористатися даною вразливістю при побудові атаки розпізнавання ключа.

ВИСНОВКИ

В результаті роботи було проведено огляд опублікованих джерел за тематикою дослідження, а саме: було розглянуто модель розпізнавача на відомих ключах, що використовує властивості ланцюгів підпросторів для блокового шифру *AES*, елементи, з яких він складається та стратегію їх роботи.

Надалі було побудовано модель розпізнавача на відомих ключах, що використовує властивості ланцюгів підпросторів «Калина»-подібних шифрів та отримано наступні результати:

1) Побудовано модель розпізнавача на відомих ключах, що використовує властивості ланцюгів підпросторів для 5 раундів шифрування для «Калина»-подібних шифрів

2) Побудовано розширену модель розпізнавача на відомих ключах, що використовує властивості ланцюгів підпросторів для 5 раундів шифрування для «Калина»-подібних шифрів

3) Побудовано розширену модель розпізнавача на відомих ключах, що використовує властивості ланцюгів підпросторів для 7 раундів шифрування для «Калина»-подібних шифрів

В результаті побудови кожної із моделей було виявлено, що «Калина»-подібні шифри за введених нами обмежень не ведуть себе як випадкова перестановка. Слід зазначити, що для практичної реалізації побудованих моделей необхідно провести щонайменше 2^{130} обчислювальних операцій. Що свідчить про те, що побудована модель розпізнавача на відомих ключах дозволяє довести, що шифр відрізняється від випадкової послідовності, але не за поліноміальний час. Саме тому, знайдена вразливість «Калина»-подібних шифрів не є критичною на сьогоднішній день.

В майбутньому, використовуючи вже отримані результати, планується будувати статистичні ймовірності для наступних раундів

шифрування «Калина»-подібних шифрів, будувати нові моделі розпізнавачів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack. In Advances in Cryptology – CRYPTO 2011: 31st Annual Cryptology Conference,Santa Barbara, CA, USA, 2011. Proceedings, pages 206–221, 2011.

2. Lorenzo Grassi, Christian Rechberger and Sondre Rønjom "Subspace Trail Cryptanalysis and its Applications to AES" [Online]. — Режим доступу: http://eprint.iacr.org/2016/592.

3. Roman Oliynykov , Ivan Gorbenko , Oleksandr Kazymyrov et al. "A New Encryption Standard of Ukraine: The Kalyna Block Cipher" [Online]. — Режим доступу:http://eprint.iacr.org/2015/650

4. Інформаційні технології. Криптографічний захист інфомації. Алгоритм симетричного блокового перетворення: ДСТУ 7624:2014. – К.: Держспоживстандарт України, 2015. – 238 с.

5. Горбенко І.Д. Перспективний блоковий шифр "Калина" – основні положення та специфікація / І.Д. Горбенко, О.С. Тоцький, С.В. Казьміна та ін. // Прикладна радіоелектроніка. – 2007. – Т.6, №2. – С.195-208

6. Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard."Springer, 2002. ISBN 3-540-42580-2.

7. Lorenzo Grassi and Christian Rechberger "New and Old Limits for AES Known-Key Distinguishers "[Online]. — Режим доступу:https://eprint.iacr.org/2017/255.pdf

8. Henri Gilbert "A Simplied Representation of AES. In ASIACRYPT 2014, volume 8873 of LNCS, pages 200–222, 2014"[Online]. — Режим доступу:https://link.springer.com/book/10.1007/978-3-662-45611-8

9. Lars R. Knudsen and Vincent Rijmen "Known-Key Distinguishers for Some Block Ciphers. In ASIACRYPT 2007, volume 4833 of LNCS, pages 315–324, 2007."[Online]. — Режим доступу:https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=31551

10. ADVANCED ENCRYPTION STANDARD (AES)[Online]. — Режим доступу:https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

11. Коляда Марія, Яковлєв Сергій "Ланцюги Підпросторів Калина-Подібних Шифрів"[Online]. — Режим доступу:http://itcm.comp-sc.if.ua/2017/Kolyada.pdf

12. Горбенко І. Д., Долгов В. І., Руженцев В. І., Олійников Р. В., Михайленко М. С., Горбенко Ю. І., Чічмар С. В. Криптостійкість шифру «Калина». Журнал "Прикладная радиоэлектроника"2007 №2